

# FlexNet Code Insight 6.13.1

User Guide

# Legal Information

Book Name:

FlexNet Code Insight 6.13.1 User Guide

Part Number: Product Release Date: FNCI-6131-UG00 May 2019

### **Copyright Notice**

Copyright © 2019 Flexera.

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

### **Intellectual Property**

For a list of trademarks and patents that are owned by Flexera, see https://www.flexerasoftware.com/legal/intellectual-property.html. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

### **Restricted Rights Legend**

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

# Contents

1	FlexNet Code Insight Overview	. 13
	Intended Audience	13
	What It Does	14
	Why It's Needed	14
	How It Works	14
	Technical Architecture Overview	14
	Common Terminology	
	Data Organization: Teams and Projects	
	· o	
2	Roles and Responsibilities	. 21
	Roles & Responsibilities	21
3	Application Administrator Tasks	. 23
	Creating New Users	
	My Shortcuts Tab: Create a New User	
	Administration Menu: Users Option	
	Adding and Removing User Account Locks	
	Creating New Teams	29
	Creating New Projects	30
	Importing Bulk Data from an Excel Workbook	31
	Using the Scripting Feature	32
	Running an Electronic Update	33
	Running an Electronic Update Manually	33
	Using the Electronic Update Server (HTTP)	33
	Using a Local Electronic Update Archive	34
	Scheduling Automatic Electronic Updates	
	Viewing Electronic Update History	34

	Email Notifications       35         Email Event Triggers and Notifications       35
4	Owner Setup Tasks
	Configuring and Editing Your Project
	Adding and Deleting Requesters
	Editing, Adding, and Deleting Project Reviewers
	Viewing, Adding, and Deleting Policies
	Viewing and Editing Policies
	Adding a Policy
	Note about Policy Conflicts
	Copying a Policy to Create a New Policy
	Viewing Scan Engine Queues
	Generating Reports
	Generating a Project Details Report
	Generating Inventory Reports
	Conducting Research
	Searching for Components
	Component Search Tips
	Component Fields
	Component Search FAQ
	Creating a New Component
	Deleting a Custom Component
	Creating a New Component Version
	Deleting a Custom Component Version       60         Adding a New Vulnerability to a Component Version       61
	Deleting a Custom Vulnerability
	Searching for Licenses
	Editing a License
	Viewing, Adding, or Editing a New Obligation
	Creating a New License
	Adding New Licenses to Components
	Deleting a License from Components    67
5	Using My Settings and Help Functions
	My Settings
	Accessing Help
6	Conducting Audits & Reviewing Inventory
	Conducting Audits
	Reviewing Inventory
	-
	Viewing Inventory Items
	Key Inventory Page Items
	Component Details

	License Details
	License Text Comparison
	Other Inventory Page Header Items
	Inventory Item Tabbed View
	Additional Inventory Details on Tabbed Views
	Viewing Source Code Fingerprint Match Highlights
7	Performing Quick Reviews & Approving or Rejecting Inventory
	Performing Quick Reviews & Marking Inventory
	Scheduling Inventory for Full Review
8	Reconciling Inventory
	What is Reconciling Inventory?
	Associating Inventory with Component Requests
	Associating Inventory with Requests across Projects
	Unassociating a Request from an Inventory Item
	Creating a New Component Request
9	Requesting Permission to Use a Component
	Requests
	Changing the Request Form       90         Required Request Form Input Fields (Attributes)       90
	Creating a Component Request
	Viewing Requests
	Viewing Request Details
	Cloning a Request
	Cloning a Request
10	Customizing the Request Dashboard
	Adding the Assigned Date Column
11	Reviewing Pending Requests
	Pending Requests
	Reviewing Pending Requests from the My Tasks Tab
	Reviewing Pending Requests from the Requests Tab
	Resubmitting Requests
	Resubmitting Requests
12	Copying & Branching Projects
	Introduction to Project Copy Feature
	Copying a Project to Reduce Administration Effort103
	Copying a Project to Support Branching a Codebase
	Copy Type: Project Configuration Only
	Data Copied During Project Configuration Copy Operation    105
	Project Settings: Workflow

	Copy Type: Custom Project Copy	106
	Copy Type: Complete Project	107
	Data Copied During the Copy Operation	109
	Project Settings: Workflow	109
	Workspace Settings: General	110
	Workspace Settings: Detection	110
	Workspace Settings: Source Code Options	110
	Workspace Settings: Automated Analysis	110
	Workspace Settings: Software Configuration Management (SCM)	110
	Workspace Reports	110
	File Tags	110
	Groups	111
	Inventory	111
	Requests	111
	Tasks	112
	Policies	112
	Comments	112
	Pre-Copy Operations	112
	Blocking Access to Source & Target Projects During Copy Operations	112
	Post-Copy Scan	113
	Email Notification	113
	Target Project Cleanup Options after Copy	113
	About Concurrently Open Workspaces	
13		114
13	About Concurrently Open Workspaces         3 Reviewing Vulnerabilities	114
13	About Concurrently Open Workspaces	114
	About Concurrently Open Workspaces	114 115 115
	About Concurrently Open Workspaces	114 115 115 117
	About Concurrently Open Workspaces	114 115 115 117 117
	About Concurrently Open Workspaces . Reviewing Vulnerabilities. Vulnerabilities . Metadata Framework . Metadata . Administering Metadata Sections and Fields.	114 115 115 117 117 117
	About Concurrently Open Workspaces   8   8   8   8   9   Metadata Framework   Metadata   Metadata .   Administering Metadata Sections and Fields.   Adding a Metadata Section	114 115 115 117 117 117 119
	About Concurrently Open Workspaces   B   Reviewing Vulnerabilities   Vulnerabilities   Metadata Framework   Metadata   Administering Metadata Sections and Fields   Adding a Metadata Field	114 115 115 117 117 117 119 119
	About Concurrently Open Workspaces   8   8   8   8   8   9   Metadata Framework   Metadata   Metadata   Administering Metadata Sections and Fields   Adding a Metadata Section   Adding a Metadata Field   Viewing, Editing, and Assigning Metadata Values	114 115 115 117 117 117 119 119 121
	About Concurrently Open Workspaces   B   Reviewing Vulnerabilities   Vulnerabilities   Metadata Framework   Metadata   Administering Metadata Sections and Fields   Adding a Metadata Field	114 115 115 117 117 117 119 119 121
14	About Concurrently Open Workspaces   3 Reviewing Vulnerabilities.   Vulnerabilities   4 Metadata Framework   Metadata   Administering Metadata Sections and Fields.   Adding a Metadata Section   Adding a Metadata Field   Viewing, Editing, and Assigning Metadata Values   Using Public APIs to Access & Assign Metadata Field Values.	114 115 115 117 117 117 119 119 121 123
14	About Concurrently Open Workspaces   8   8   8   8   8   9   Metadata Framework   Metadata   Metadata   Administering Metadata Sections and Fields   Adding a Metadata Section   Adding a Metadata Field   Viewing, Editing, and Assigning Metadata Values	114 115 115 117 117 117 119 119 121 123
14	About Concurrently Open Workspaces   3 Reviewing Vulnerabilities.   Vulnerabilities   4 Metadata Framework   Metadata   Administering Metadata Sections and Fields.   Adding a Metadata Section   Adding a Metadata Field   Viewing, Editing, and Assigning Metadata Values   Using Public APIs to Access & Assign Metadata Field Values.	114 115 115 117 117 117 119 119 121 123 125
14	About Concurrently Open Workspaces   3   Reviewing Vulnerabilities.   Vulnerabilities   4   Metadata Framework   Metadata.   Administering Metadata Sections and Fields.   Adding a Metadata Section   Adding a Metadata Field   Viewing, Editing, and Assigning Metadata Values   Using Public APIs to Access & Assign Metadata Field Values.	114 115 115 115 117 117 117 119 119 121 125 125
14	About Concurrently Open Workspaces   8   8   8   8   8   9   Metadata Framework   9   Metadata   Administering Metadata Sections and Fields   Adding a Metadata Section   Adding a Metadata Field   Viewing, Editing, and Assigning Metadata Values   Using Public APIs to Access & Assign Metadata Field Values   5   Using the Product Catalog	114 115 115 115 117 117 117 119 119 121 125 125 125
14	About Concurrently Open Workspaces         3       Reviewing Vulnerabilities         4       Metadata Framework         4       Metadata Framework         4       Metadata A         Administering Metadata Sections and Fields         Adding a Metadata Section         Adding a Metadata Field         Viewing, Editing, and Assigning Metadata Values         Using Public APIs to Access & Assign Metadata Field Values         5       Using the Product Catalog         The Product Catalog         Associating Requests to Product Catalog Items	114 115 115 115 117 117 117 119 119 121 123 125 125 125
14	About Concurrently Open Workspaces         3       Reviewing Vulnerabilities.         Vulnerabilities         4       Metadata Framework         Metadata         Administering Metadata Sections and Fields.         Adding a Metadata Section         Adding a Metadata Field         Viewing, Editing, and Assigning Metadata Values         Using Public APIs to Access & Assign Metadata Field Values.         5       Using the Product Catalog         The Product Catalog         Associating Requests to Product Catalog Items.         Associating Inventory with Requests Across Projects.	114 115 115 115 117 117 117 119 119 121 123 125 125 125 125 125 125
14	About Concurrently Open Workspaces         Reviewing Vulnerabilities         Vulnerabilities         Metadata Framework         Metadata         Administering Metadata Sections and Fields.         Adding a Metadata Section         Adding a Metadata Field         Viewing, Editing, and Assigning Metadata Values         Using Public APIs to Access & Assign Metadata Field Values.         5         Using the Product Catalog         The Product Catalog         Associating Requests to Product Catalog Items.         Associating Inventory with Requests Across Projects.         Generating Third-Party Notices for Requests based on Product Catalog Items.	114 115 115 115 117 117 117 119 119 121 123 125 125 125 126 126
14	About Concurrently Open Workspaces         Reviewing Vulnerabilities.         Vulnerabilities         Metadata Framework         Metadata         Administering Metadata Sections and Fields.         Adding a Metadata Section         Adding a Metadata Field         Viewing, Editing, and Assigning Metadata Values         Using Public APIs to Access & Assign Metadata Field Values.         Using the Product Catalog         The Product Catalog .         Associating Requests to Product Catalog Items.         Associating Inventory with Requests Across Projects.         Generating Third-Party Notices for Requests based on Product Catalog Items.         Reporting on Findings Based on Product Catalog Items	114 115 115 115 117 117 117 119 119 121 123 125 125 125 125 126 126
14	About Concurrently Open Workspaces         8       Reviewing Vulnerabilities.         Vulnerabilities         4       Metadata Framework         Metadata       Administering Metadata Sections and Fields.         Adding a Metadata Section       Adding a Metadata Field         Viewing, Editing, and Assigning Metadata Values       Using Public APIs to Access & Assign Metadata Field Values.         5       Using the Product Catalog         The Product Catalog       Associating Requests to Product Catalog Items.         Associating Inventory with Requests Across Projects.       Generating Third-Party Notices for Requests based on Product Catalog Items.         Reporting on Findings Based on Product Catalog Items       Administering the Product Catalog.	114 115 115 115 117 117 117 119 119 121 123 125 125 125 125 126 126 126
14	About Concurrently Open Workspaces .         8       Reviewing Vulnerabilities.         Vulnerabilities         4       Metadata Framework         Metadata .         Administering Metadata Sections and Fields.         Adding a Metadata Section         Adding a Metadata Field         Viewing, Editing, and Assigning Metadata Values .         Using Public APIs to Access & Assign Metadata Field Values .         5       Using the Product Catalog .         The Product Catalog .         Associating Requests to Product Catalog Items.         Associating Inventory with Requests Across Projects.         Generating Third-Party Notices for Requests based on Product Catalog Items.         Reporting on Findings Based on Product Catalog Items.         Administering the Product Catalog.         Projects.	114 115 115 115 117 117 117 119 121 123 125 125 125 125 126 126 126 126 126 126 127

Viewing, Editing and Associating Product Catalog Items	. 128
Associating Product Catalog Items with a Project	. 129
Associating Product Catalog Items with a Request	. 130
Associating Inventory with Requests across Projects	. 131
Reporting on Requests (Filtered by Product Catalog)	. 132
Reporting on Third-Party Notices for Requests (Filtered by Product Catalog)	. 133

16	Performing Advanced Searches.	135
	Advanced Searches	. 135

Project Advanced Search	
Inventory Advanced Search	
Request Advanced Search	
Component Advanced Search	
License Advanced Search	
Policy (Web UI) Advanced Search	
Team (Web UI) Advanced Search	
Group (Detector) Advanced Search	
Advanced Project Search Example	

17	FlexNet Code Insight Public A	Pls.	• • • •												• • •		• • •	139	3
----	-------------------------------	------	---------	--	--	--	--	--	--	--	--	--	--	--	-------	--	-------	-----	---

Public API Entry Points and Contexts	139
Accessing Core & Scan Servers via ScriptRunner	140
API Covers (Facades)	142
Admin Service Cover	
Metadata Service Cover	
Reference Data Service Cover	
Project Data Cover	
Auditor Service Cover	
Workspace Locator Cover	
Workspace Cover	

18	Auditing and Analysis Overview	147
	Tasks an Auditor Performs	. 147
	How Auditors Perform Tasks	. 148
	Why Auditors Perform Tasks	. 149

<b>19</b>	Configuring Workspaces	151
	Workspaces	151
	Accessing Workspace Configuration Settings	151
	General Tab Tasks	153
	Software Configuration Management Tab	154
	Detection Tab Tasks	155
	Source Code Options Tab	156
	Rescan Options Tab	157

	Automated Analysis Tab
20	Automated Analysis 161
	POM File Analyzer
	Auto-WriteUp <sup>™</sup>
	Multi-Indicator Detector (MID)
	Analyzer
	CodeAware
	Comparison of the Analysis Techniques
21	Using Auto-WriteUp <sup>™</sup>
	Auto-WriteUp <sup>™</sup>
	Enabling Auto-WriteUp <sup>™</sup>
	Detection Rules
	Configuring Auto-WriteUp <sup>™</sup> 169
	Frequently Asked Questions
	Workspace Backup/Restore Scripts    173      Troubleshooting    173
22	Workspace Scanning & Report Scheduling 175
~~	Scheduling a Scan
	Generating a Report
23	Workspace Resources    177
	Accessing Workspace Resources
	Editing Workspace Settings
	Launching Detector
	Viewing Tasks in Queue for a Workspace
	Viewing Reports for a Workspace
24	Workspace Operations 181
	Accessing Workspace Operations
	Renaming a Workspace
	Copying a Workspace
	Deleting a Workspace
25	Using the Analyzer 183
	The Analyzer
	Requirements
	Reports
	Permissions.
	Running the Analyzer

	FlexNet Code Insight Data Services
	Ports
	Setup
	Performing a Quick Assessment with the Analyzer185
	Auto-creating Component Groups with the Analyzer 186
	Administration
	Updates
	Settings
	Core Settings
	Project Settings
	Frequently Asked Questions
26	Accessing a Workspace to Analyze 191
	Accessing Workspaces
27	Viewing and Updating Scheduler Queuing 193
	Viewing the Scheduler Queue
28	Launching Detector & Viewing Scan Results
	Opening Detector to View Scan Results
	Detector Tabs and File Tree Views
29	Viewing Evidence
	Viewing Evidence
	Types of Evidence
	Filtering the File Tree
	Displaying Only Desired Files (Nodes)
	Displaying Only Exact Matches
	Displaying Partial Matches
	Displaying Copyrights
	Displaying Emails & URLs
	Displaying License Matches
	Displaying Search Term Matches
	Displaying Source Code Fingerprint (SCF) Matches
	Displaying Source Code Fingerprint (SCF) Matches
	Displaying Java Name Matches
	Viewing SCM File Check-In History
30	Analyzing Files with Evidence (Third-Party Indicators)
	About Analyzing Files With Evidence
	Researching a File
	Designating Files That Have Been Reviewed
	Tagging Files and Archives
	Tagging a File

Tagging an Entire Directory	
Assigning a Different Value to a Tag	
Filtering Files and Results	
Filtering Files	
Filter Expression Options	
Custom Script-Based Filters	

31	Managing Inventory via Groups	225
	About Groups	. 225
	Managing Groups	. 226
	Creating a Group	. 226
	Deleting a Group	. 227
	Copying an Existing Group	. 227
	Managing Group Details	. 228
	Managing Third-Party Notices Data for a Group	. 229
	Adding or Editing Group Details	. 231
	Setting Group Status Information	. 232
	Managing Licenses for a Group	. 232
	Viewing Groups Created by System	. 233
	Creating User Groups	. 234
	Adding Files to a Group	. 234
	Publishing Groups	. 236
	Recalling Groups	. 236
	Recalling a Group from the Individual Group Pane	. 236
	Recalling Groups Bulk Fashion	. 236
	Viewing and Confirming Published Inventory	. 237

32	Working with Archives	239
	Supported Archive Types	. 239
	Types of Evidence	. 239
	Source Matches	. 240
	Exact Matches	
	Viewing Evidence	. 240
	Groups	. 241
	Tags	. 242
	Archive File Counts/Nested Archives	. 243
	Tagging an Archive for Scanning	. 244
	Archive File Operations	. 244
	Directory Operations for Archives	. 245
	Bulk-File Operations for Archives	. 245
33	Using Multi-Select for Bulk Operations	247

34	Detector Code Search
	Detector
	Code Search Indexing
	Disabling Code Search Indexing
	Launching Code Search
	Using the Code Search Icon
	Using the File Context Menu: File Name Search
	Using the Partial Matches Panel String Search251
	Code Search Examples
	Special Characters
	Using Code Search for Binary Files
	Customizing Code Search Indexing
	Detector Code Search APIs
35	Generating Custom Fingerprints 257
	Custom Fingerprints
	customFingerprints.groovy Options
36	Upload to Scan
	Configuring Upload to Scan
	core.properties
	scanEngine.properties
	Prerequisites
	Supported File Types
	File Permissions
	Upload Size
	Using Upload to Scan
	Limitations
	Error Handling
	Security Features
	Core Server

Contents

```
1
```

# **FlexNet Code Insight Overview**

This section provides an overview of FlexNet Code Insight.

- Intended Audience
- What It Does
- Why It's Needed
- How It Works
- Technical Architecture Overview
- Common Terminology
- Data Organization: Teams and Projects

## **Intended Audience**

The FlexNet Code Insight 6.13.1 User Guide is intended for the following team members:

- Developers
- Technical leads, senior engineers
- Engineering managers
- IT security officers
- Project managers
- Release managers
- Program managers
- Legal and patent attorneys

## What It Does

FlexNet Code Insight is the industry's first application security solution targeting today's widespread use of Open Source Software (OSS). FlexNet Code Insight leverages the industry-leading detection and analysis capabilities of Flexera products by integrating a policy-based software component-management system with inventory, for example, intellectual property in the form of published groups of files via Detector.

Role-based features and functions help engineering and project management streamline daily code management activities for various team members. Hierarchical organization creates an effective and accurate view of team projects and software use policies.

# Why It's Needed

If your company is concerned about any of the following, you need FlexNet Code Insight:

- GPL and other Viral Licenses (especially v3.0)
- Affero GPL
- Commercial Content and Libraries
- Restrictions on commercial use or field of use (e.g. no Military use)
- Cryptography
- Code with Unknown Licenses
- Percent (%) of undisclosed content

### **How It Works**

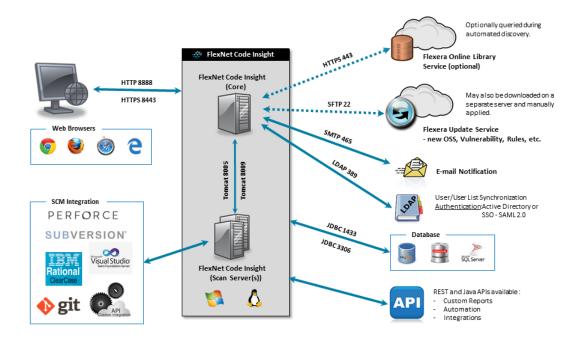
Flexera's unique software composition analysis technology captures the composition of a code base, and provides your team with an inventory of Open Source software (OSS) component usage. The resulting inventory identifies security vulnerabilities and intellectual property (IP) issues associated with the inventoried OSS components.

The policy and code management workflow of FlexNet Code Insight enables development organizations to cost effectively manage and secure mission critical applications and products.

Component management tasks are assigned and completed by a cross-functional team of users in line with the policies of FlexNet Code Insight.

## **Technical Architecture Overview**

The following diagram shows how the various clients work in conjunction with the workspaces, databases, and the FlexNet Code Insight application. FlexNet Code Insight implements the code management workflow on top of inventory detection, analysis, and generation capabilities.



# **Common Terminology**

The following are common terms that appear in FlexNet Code Insight documents and on reports and product pages:

Terms	Definitions
AutoWriteUp - Ibiblio Maven2	Uses component information from the bulk collection of metadata from a Maven mirror to create inventory items for jars.
CL	Compliance library, a collection of data that FlexNet Code Insight uses to generate an inventory of vulnerabilities. This library is large and is provided on a separate disk.
Component Analyzers	The analyzers identify source distributions of common open source projects, especially targeting those in the C/C++ where package managers and metadata files are not standard. These analyzers are attuned to regularities across the entire history of the open source project, so generally even a version released tomorrow can be identified reliably. Other Analyzers identify packages and components from widely used package managers and repositories.
Component Analyzer - Abstracted	This Analyzer leverages the high-quality data of a component analyzer when that component is found in other, non-source-code contexts (such as binary distributions).

Terms	Definitions
Composer (php) Package Analyzer	An analyzer for Composer (php) packages. If there is a composer.lock file, those defined dependencies and versions will be used. If there is no lockfile (e.g. if the package has not been 'installed'), then composer.json files are parsed for uninstalled 'required' dependencies ( <b>Uninstalled Composer Dependency</b> ). In this case, versions are set at the most recent version in the Packagist registry (packagist.org) that satisfies the given composer.json's semantic versioning restrictions ( <b>Composer/Packagist API</b> ).
CPE	Common Platform Enumeration, a widely-used, standard methodology to define and distinguish such items as application classes, operating systems, and hardware present in a organization's computing environment.
CRAN Analyzer	Uses metadata within a CRAN source code package to create an inventory item.
CVE	Common Vulnerabilities and Exposures, a list of known information-security vulnerabilities and exposures in commercial and open-source software. Hackers can use software errors and software code errors to gain access to a company's computer systems. For more information, visit http://cve.mitre.org/.
Data Services - Component Lookup	Uses Data Services to look up the best FlexeNet Code Insight component match.
Data Services - Digest	Use a file's md5 digest to determine whether the file has an Auto-WriteUp rule or other library data associated with it.
Data Services - Maven Component Lookup	Uses GroupId and ArtifactId to select the best FlexeNet Code Insight component.
Data Services - Release Name	Uses Data Services to analyze the origin of the file based on library collection data.
GPL	General Public License. These licenses for open source code expose commercial code that contains open source to public copyright.
Intellectual Property (IP)	Refers to creations of the intellect for which a monopoly is assigned to designated owners by law. In the context of FlexNet Code Insight and this guide, IP refers to programming code created internally or externally.
Intellectual property rights (IPRs)	Legal protections, such as trademark, copyright and patents, given to the owners and/or creators of IP.
Inventory	A list of all available OSS components. Inventory takes the form of published groups from the Detector, the result of auditing analysis.

Terms	Definitions
JDBC Driver Connector File	A file required to establish a connection with your data source. You must specify this file during installation.
Jenkins	A Java open source automation server that supports continuous integration.
License Lookup - Component Level	Identifies the license(s) of a component across versions. Typically this will be an aggregate of the licenses for the project over time or the license at the time of data collection.
License Lookup - Version Level	Identifies the license(s) of a component at a specific version. This data is sensitive the possibility of a change in license over time.
LOC	Lines of Code.
NPM Analyzer	Identifies node_modules from npm and other components using a package.json file to store metadata.
OSS	Open Source Software.
Policies	Rules and conditions assigned globally or to specific teams or projects which automate the review process of inventory items and/or requests to use OSS components.
РОМ	Project Object Model
POM Analyzer	An analyzer that analyzes pom.xml files to determine dependencies and resolve versions based on the project's declared or inherited properties. The Analyzer will attempt to retrieve pom information about dependencies from the local maven repositories (as defined in the pom.xml) or Maven Central. To become an inventory item, dependencies must:
	• have a version that can be resolved
	not be in scope Test
	not be set to Optional
POM Ancestry License	Indicates a license determined by the declared license in a parent POM file.
POM Dependency	A GroupId ArtifactId pair identified as a dependency within a pom.xml file. See POM Analyzer for the conditions under which a dependency will become an inventory item.
POM License Declaration	Indicates a license determined by the declared license in the POM.
POM Transitive Dependency	A dependency not declared directly in a project's POM, but inferred from the retrieved POM of a dependency.
POM <type> Copyright</type>	Indicates various methods for building a copyright for the purpose of creating a notice.

Terms	Definitions
Projects	Specific development goals, usually a software application or element that a project team is developing. Projects are comprised of workspaces, policies, requests, inventory, and tasks.
Related Component Lookup	Improves component information, such as CVEs and License data, by finding different FlexeNet Code Insight components for the same Open Source project as found in different forges (e.g. the component that corresponds to the RPM's centos distribution and the SourceForge source repository).
Reports	Project- or inventory-based lists of code, license citations filtered by global, team, or project parameters.
Requests	Inquiries from users asking if certain third-party code or components are allowable for use in their software development projects.
RPM Metadata	Uses metadata store inside an RPM to create an inventory item.
RubyGem Analyzer	Uses metadata within a RubyGem package in source code form to create an inventory item.
RubyGems API	Indicates that the RubyGems.org API (rubygems.org) was used to get metadata about a .gem package to create an inventory item.
SCA	Software Composition Analysis.
Tasks	Individual actions in the code management workflow.
Uninstalled Node Module Dependency Inventory	When there is a package.json with dependencies but the corresponding node modules are not installed. The NPM API uses the npm registry (registry.npmjs.org) to get package information and resolve semantic versioning. Versions are set at the most recent version in the npm registry that satisfies the semantic versioning restrictions in the given package.json file.
Users	Those accessing the application on a frequent or infrequent basis with roles and responsibilities that have been assigned to them by the application administrator and project owner.
Viral license	A derogatory term synonymous with copyleft license, itself a play on the term "copyright." In general, if your codebase contains open source code, you are required to retain a copyright statement that contains license terms and author acknowledgment in any application or software derived from your codebase. In addition, any codebase containing code covered by a viral license must be provided for free.
Workspace	A container for codebase scan settings and scan results. A project may contain multiple workspaces which together comprise the entire codebase for that project.

# **Data Organization: Teams and Projects**

Global data is comprised of teams. Teams are comprised of projects, and projects are comprised of workspaces:



- Global assignment: The policy or rule is applied to any and all teams within the corporation that use this application; for example, a corporate-wide standard.
- Team assignment: An organizational unit is influenced by a policy or rule; for example, all software development teams working within the corporation, regardless of the project.
- Project assignment: Only a specific project is influenced by a policy or rule; for example, only the widget API version 1.14 release is influenced by the policy or rule.

Chapter 1 FlexNet Code Insight Overview

Data Organization: Teams and Projects



# **Roles and Responsibilities**

This section includes the following topic:

• Roles & Responsibilities

## **Roles & Responsibilities**

The following Set Up and Code Management Tasks table provides a summary of the FlexNet Code Insight process and shows which roles are eligible for which activities.

FlexNet Code Insight requires some application administrative setup tasks. Then all of the ongoing code management cycle tasks occur in parallel. Users can perform any function appropriate to their assigned roles and the progress of the project.

FlexNet Code Insight includes automatic approval and rejection features to facilitate efficient responses to requesters, as well as a manual review feature.

- Automatic Acceptance: The automatic acceptance feature of the policy engine gives developers and other requesters an immediate answer as to which components are already approved for use. This is useful, for example, for setting up pre-approved versions of a corporate repository.
- Automatic Rejection: This feature gives requesters an immediate answer when users request known unacceptable components. Automatic rejection is useful for quickly communicating inappropriate license/usage combinations and unsecured components.
- Manual Review: This feature allows employees with the appropriate permissions to review component requests, which may have varying restrictions and need to be reviewed on a case-by-case basis. We suggest that the policy administrator set the Review policy before allowing users to access the application's features.

These features allow users to see the policies and rules in real time as they make requests and perform reviews related to specific projects. However, you can also do this after users have accessed the system.

Task	Category	Milestone Target	Role	Activity
Setting up and Configuring a	Create Project	Project start	Application Admin	Create users, teams, projects
Project	Review Project Policy	Project start, Ongoing	Policy Admin	<ul> <li>Define conditions of use</li> <li>Add attachments to policies</li> <li>Manage project policies</li> </ul>
	Configure Project	Project Start	Participant (selected as the Project Owner)	Set project users roles, such as assign auditor and security analyst Define request review process Associated workspaces with project
Code Management Cycle	Conduct Audit	Ongoing	Auditor	Audit codebase associated with project and publish groups to create inventory items
	Create Component Requests	Ongoing	Requester	Create requests, review and acknowledge conditions of use imposed by reviewers
	Review a Request	Ongoing	Reviewer	Review requests and define conditions of use (technical, business, legal, etc.)
	Reconcile Inventory	Ongoing	Owner or project participant	Review project inventory detected via audit and associate with request approving its use
	Security Review for Vulnerabilities	Ongoing	Project Security Analyst	Review vulnerabilities associated with project inventory detected via audit
	Report Generation	Ongoing	Various	Capture a summary of inventory or security cycle status to share with project team

#### Table 2-1 • Set Up and Code Management Tasks

# **Application Administrator Tasks**

The application administrator can enter user, team, and project data into FlexNet Code Insight. The user with this role has to possess a data-entry skill set. The application administrator is responsible for completing the following activities at the start of a project:

- Creating New Users
- Creating New Teams
- Creating New Projects
- Importing Bulk Data from an Excel Workbook
- Using the Scripting Feature
- Running an Electronic Update
- Email Notifications

### **Creating New Users**

The following are the ways to add users to projects:

- My Shortcuts Tab: Create a New User
- Administration Menu: Users Option

### My Shortcuts Tab: Create a New User

You can create new users from the My Shortcuts tab.



#### To create a new user, do the following:

1. Log into FlexNet Code Insight as administrator:

Username	admin	
Password	•••••	•
		Login

The Administration Home page appears. On this page you can create users, teams, and projects.

S Home   🍈 Administration 🕶			() H
G Home			
New request	O requests submitted by me	<b>0</b> requests assigned to me	Search requests
My Shortcuts Create a new user Create a new team			
Create a new team Create a new project			

- 2. You may also use the Main menu bar to navigate the administration pages.
- 3. To create new users, click **Create a new user**. The **User Details** page appears:

🚱 Home 📔 🎲 Administration	<b>•</b>		() н	lelp
🗞 User Details				
* Login		System Administrator		
* First Name		Policy Administrator		
Middle Name		 Scripting Administrator		
	_	 Requester		
* Last Name	_	Reviewer		
* Email		Participant		
Job Title				
Business Unit				
Location				
Telephone				
Facsimile				
* Login Question				
* Login Answer				
Lock Account				
Generate Password				

- **4.** Enter all necessary user information and set the role of the user by checking one of the possible project roles in the shaded box to the right. FlexNet Code Insight sends automatic emails to new users notifying them of the system-generated temporary password. New users will be prompted to change this password the first time they log in. Ensure that you enter a valid email address for each user.
- 5. Click Save to save your changes.

### **Administration Menu: Users Option**

The other way to add and manage users is via the Administration pull-down menu. This allows you to manage users in your system as well as integrate with an LDAP server to dynamically populate a user list.



To add and manage users via the Administration pull-down menu, do the following:

- 1. Log into FlexNet Code Insight as an *administrator*.
- 2. Click Administration button on the Main menu bar.
- Select Users from the pull-down menu. The Users Administration page appears. The User tab allows you to manage users, while the User Lists tab allows you to manage user lists. Follow the steps in My Shortcuts Tab: Create a New User to manage a single user.

Users User	Lists					
Search:		Q			0	Add New User
Login »	First Name	Last Name	Email	Roles	Last Updated	Actions
admin			admin@admin.com	System Administrator	09/21/2015	20
dev1	Developer	One	devnul@palamida.com	Requester	09/25/2015	20
dev2	Developer	Two	devnuli@palamida.com	Requester	09/25/2015	20
dev3	Developer	Three	devnull@palamida.com	Requester	09/25/2015	20
dev4	Developer	Four	devnul@palamida.com	Requester	09/25/2015	20
dev5	Developer	Five	devnuli@palamida.com	Requester	09/25/2015	20
legal1	Legal	One	devnull@palamida.com	Requester Reviewer	09/25/2015	20
legal2	Legal	Two	devnuli@palamida.com	Requester Reviewer	09/25/2015	20
legal3	Legal	Three	devnull@palamida.com	Requester Reviewer	09/25/2015	20
legal4	Legal	Four	devnull@palamida.com	Requester Reviewer	09/25/2015	20

4. To manage user lists, select the User List tab, and then click the Add New User List icon. The User List Details page appears:

Name	ldap_users			
Description				
User List Type	Mixed			*
LDAP Query	All employees w	ill be associated with this us	er list.	
Users	Search:		Q	

- 5. Enter the name and description for the User list.
- **6.** To filter the available users to only ones with the required role, select one of the following user types from the User List Type pull-down menu:

**Note** • You cannot change the user list type after creation so be sure to select the rightone.

- Mixed: All users can be associated with this type of user list. User list cannot be associated with a project role on the project configuration page.
- **Project Participant**: Only users with the project participant role can be associated with this type of user list. This user list can be associated as project observers, auditors, security analysts, or QuickReview facilitator on the project configuration page.

- **Requester**: Only users with the requester role can be associated with this type of user list. This user list can be associated with the requester role on the project configuration page.
- **Reviewer**: Only users with the reviewer role can be associated with this type of user list. This user list can be associated with any review level on the project configuration page.
- 7. If LDAP has been enabled, and if the User List LDAP properties have been properly defined in the core.ldap.properties configuration file, the user list is dynamically updated during each LDAP sync to contain users returned by the LDAP query. If a user list has been configured to utilize an LDAP query rather than be manually populated, the description of the associated LDAP query will be shown, and the add/delete users buttons will no longer be available to manually manage users for this user list. Users with mismatched roles (based on the user list type) will be removed from the list returned by the LDAP query.
- **8.** The following parameter must be configured to set user role assignment during the LDAP sync. The available roles are: requester, reviewer and participant. All other roles must be set manually. See the "LDAP Configuration" section of the *Installation and System Administration Guide* for more detailed instructions on configuring this property.

```
ldap.user.role = requester, reviewer, participant
```

**9.** The following two parameters must be configured for each user list that is associated withan LDAP query. The LDAP query will be executed each time an LDAP syncoccurs.

```
<userlist_name>.ldap.description
```

A human-readable description of the LDAP query. This will be shown on the **User List Details** page to indicate to the user which LDAP query is dynamically being used to populate the user list.

<userlist\_name>.ldap.query

The LDAP query to execute for fetching users to dynamically populate the associated user list.

**10.** You can also manually associate any user with the necessary roles to a user list via the Users table. Click in Add Users to select the Users to add to the User List or remove existing users via the checkbox to the left of the name and then click on the **Delete Users** button.

User List Details				
Name	Requesters			
Description				
User List Type	Requester			×
Users	Search:		Q	🔇 Delete Users 🛛 O Add Users
	🔲 login	First Name 🔺	Last Name	Email
	🔲 elex	Alex	Rybak	arybak@palamida.com
	requester1	Requester1	One	user@email.com
	requester2	Requester2	Two	user@email.com
	requester3	Requester3	Three	user@email.com
	requester4	Requester4	Four	user@email.com
	requester5	Requester5	Five	user@email.com
	requester6	Requester6	Six	user@email.com
	requester7	Requester7	Seven	user@email.com
	requester8	Requester8	Eight	user@email.com
	requester9	Requester9	Nine	user@email.com
	14 4 Page	1 of 1   🕨 🕅 🖉   Show	All	1 - 10 of 1

**11.** If you have LDAP configured, you can sync FlexNet Code Insight with LDAP at any time by going to the User Sync tab and pressing the Start User Sync button. This will dynamically update all users and user lists in the system. For more information on how to configure LDAP, see the "Integrating with LDAP for Authentication (Optional)" section in the *FlexNet Code Insight Installation and System Administration Guide*.

### Adding and Removing User Account Locks

The system locks out someone who repeatedly attempts to access the system with incorrect login and password information. If this occurs, users will see the following message:

Login failed, please verify your username and password.

As an administrator, you may also lock a suspicious user out of the system.



#### To lock or unlock a user account, do the following:

- 1. Log in to FlexNet Code Insight as *administrator*.
- 2. Select Users from the Administration pull-down.
- 3. Click the pencil and paper icon associated with a user name or on the appropriate link in the Login column.
- 4. Lock or unlock a user account:
  - To lock a user account, check **Lock Account**.
  - To unlock a user account, uncheck Lock Account.

Login	palamida	System Administrator	1
First Name	Juliya	Policy Administrator	1
Middle Name		Scripting Administrator	1
Last Name	Rubin	Requester	V
Email	jrubin@palamida.com	Reviewer	V
Job Title		Participant	V
Business Unit		1	
Location		1	
Telephone		1	
Facsimile		1	
Login Question	question	]	
Login Answer	answer	]	
Lock Account	V		
Generate Password			
Password	•••••		
Confirm Password		]	
		Save Cancel	

Note • The lock/unlock options are not available for external users (i.e., LDAPusers)

5. Click Save.

# **Creating New Teams**

Î

Task

#### To create a new team, do the followings:

- 1. Click Home in the top left-hand corner to return to the Administrator Home page.
- 2. Click the **Create a new team** link. The **Team Details** page opens. You may also use the Administration → Teams command on the Main Menu bar to navigate the administration pages.

Team De	tails				
General	ClearCase Restrictions	Scan Folders Restrictions			
Name					
Descrip	otion				
Team M	Aetadata 🛛	Create Team Metadata			

**Note** • To use the Create Team Metadata button, you must have created Metadata fields for Teams. To create metadata, log in as Administrator, and see the Metadata command on the Administration pull-down menu. Metadata is typically

4. If ClearCase has been enabled for any scan servers, a ClearCase restrictions tab will be shown on the Team Details

created during the system configuration phase. However, it can also be created any time thereafter.

3. Enter a team name and a team description in the General tab.

Team Details					
	Restrictions Scan Fold	ers Restrictions			
Scan Server	[				
ClearCase Views	Available ClearCase Vie	ews	Allowed	ClearCase Views for this Team	
	-	Apply Filter	Remove Filter	Add View	Remove Selected Views
			-		
ClassCase VOPs	_	iews to Allowed List for T		Clauces 100 for this Tarr	
ClearCase VOBs	Add Selected V Available ClearCase VO	Bs		ClearCase VOBs for this Team	Remove Selected VOB
ClearCase VOBs	_		Allowed		Remove Selected VOBs

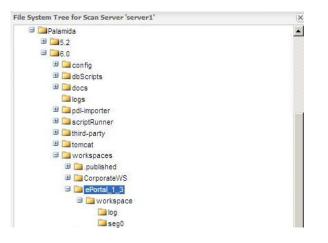
This tab is used to restrict which ClearCase views and VOBs may be used for scanning by all projects under this team.

- A filter may be used to find the desired views and/or VOBs.
- Selected views and VOBs will be saved with the team, and will restrict available values in the Workspace Settings
  page for the Project Owner and Auditor.

- The clearcaseRestrictionsShowAllDataByDefault property in the scm.properties file controls whether all views and VOBs are shown to the Project Owner and Auditor on the Workspace Settings page if no ClearCase restrictions have been defined for the team. By default, the property is set to true, so all ClearCase views and VOBs are available unless restricted by the ApplicationAdministrator.
- 5. The Scan Folder Restrictions tab is used to restrict which locations on the scan server may be used for scanning by all projects under this team.
- 6. Select the Scan Server from the pull-down menu.
- 7. Click **Browse** to select folders from the server file system tree, or manually type in the full path, as shown in the following figure.

eneral	ClearCase Restrictions	Scan Folders Restrictions	
<ul> <li>Scan Server</li> <li>Folders to Scan</li> </ul>		server1	
			Browse
			Туре
			Remove

8. In the server file system tree, select the scan server to display that server's file system tree.



- **9.** Click on the folder(s) to add them to the list of locations that can be selected in the workspace settings for any project under this team. This will restrict which folders can be scanned for all projects under this team.
- 10. Click the Save button.

# **Creating New Projects**

 Task
 To create a new project, do the following:

1. To the Administrator Home page click the Home button in the top left-hand corner.

2. Select the Create a new project link. The Project Details page appears:

Name		
Description		
Team	Select a team	×

You may also use Administration → Project command on the Main menu bar to navigate to the administration pages.

- **3.** On this page, enter the following:
  - Name: Name of the project
  - Description: Brief description of the project
  - Team pull-down menu: Select the team to which this project belongs
  - Owner pull-down Menu: The project owner. Project owners have permission to create, delete, and modify certain types of data.

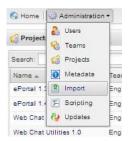
## **Importing Bulk Data from an Excel Workbook**

The Bulk Import feature allows you to import data globally. For example, you can bulk import all requests as completed.

Task

To bulk import user, simple policy, or completed request data via an Excel Workbook (spreadsheet), do the following:

- 1. Access the Admin Home page by clicking on the Home button in the top left-hand corner.
- 2. Click the Administration pull-down menu:



3. Select the Import option. The Import page appears:

🚱 Home 🛛 🌍 Administration 🔹		Welcome Admin	🔐 My Settings	🛟 Help   ┥	Logout
1 Import					
Browse	Import				
Download a sample workbook for bulk license obligations import					
Download a sample workbook for bulk policy import					
Download a sample workbook for bulk request import					
Download a sample workbook for bulk user import					

On this page, click **Browse** to select a system data file to import.

4. If you click **Download**, a sample workbook for bulk user import, an Excel workbook sample page opens populated with sample FlexNet Code Insight administration data:

File Hom	e Insert	Page Layout	Formula	Data Rev	view View	Acrobat						
			🛛 Ruler	Formula Bar				Split	View Si	de by Side onous Scrolling		27
		istom Full	Gridlines	Headings		coom to New election Windo	Arrange Free	ze		Vindow Position	Save	Switch e Windows
	rkbook Views	iews sereen		Show	Zoom	cicculon minuo	w an run		Window		workspuce	
	TROOOK VIEWS			311044	20011				WINDOW			
A1	+ (**	∫x ∪	ISERS									
A	В	C	D	E	F	G	н	I J	К	LM	N	0
1 USERS										ROLES A	ND PRIVILE	GES
2 Login	First Name	Middle Name	Last Name	Email	Security Questio	Security Answe	Telephone  F	ax Business Un	i Locatior Je	ob TitleRequeste	Reviewer	roject Part
3 superuser	Super	(superuser)	User	user@email.com	company	palamida	415-555-1212			X	X	X
4 observer	Observer	(observer)	Smith	user@email.com	company	palamida	415-555-1212			1		X
5 owner	Owner	(owner)	Smith	user@email.com	company	palamida	415-555-1212	8	-		8	X
6 auditor	Auditor	(auditor)	Smith	user@email.com	company	palamida	415-555-1212	2		1	£ 1	X
7 security_analy.	st Security	(security analyst		user@email.com	company	palamida	415-555-1212	1				X
8 policy_admin	Policy	(admin)	Admin	user@email.com	company	palamida	415-555-1212					
9 requester1	Requester1	(requester)	One	user@email.com	company	palamida	415-555-1212			X		
10 requester2	Requester2	(requester)	Two	user@email.com	company	palamida	415-555-1212			X		
11 requester3	Requester3	(requester)	Three	user@email.com	company	palamida	415-555-1212			×		
12 requester4	Requester4	(requester)	Four	user@email.com	company	palamida	415-555-1212			×		
13 requester5	Requester5	(requester)	Five	user@email.com	company	palamida	415-555-1212	8		×	8. B	
14 requester6	<b>Requester6</b>	(requester)	Six	user@email.com	company	palamida	415-555-1212	1		8	2 1	
15 requester7	Requester7	(requester)	Seven	user@email.com	company	palamida	415-555-1212	8		×	e 8	
16 requester8	Requester8	(requester)	Eight	user@email.com	company	palamida	415-555-1212			X		
17 requester9	Requester9	(requester)	Nine	user@email.com	company	palamida	415-555-1212			×		
18 reviewer1	Reviewer1	(reviewer)	One	user@email.com	company	palamida	415-555-1212				X	
19 reviewer2	Reviewer2	(reviewer)	Two	user@email.com	company	palamida	415-555-1212				×	

# **Using the Scripting Feature**

Task

To access the scripting feature, do as follows:

1. Access the **Admin Home** page by clicking the Home button in the top left-hand corner. Access the scripting feature from the **Administration** pull-down menu:

2	Users
-	Teams
3	Projects
0	Metadata
	Import
F	Scripting
82	Updates

#### The **Scripting** page appears:

🔁 Scripting			
Select a script to execute	¥	Excute Script	

- 2. Select a script from the pull-down menu.
- 3. To execute the selected script, click Execute Script.
- **4.** The scripts are registered in the database (MySQL/Oracle) using the following sample insert statement. The corresponding groovy script file should be placed in the scripts directory under the following:

```
$Code Insight_ROOT_DIR/config/core/scripts/.
INSERT INTO pas_system_script (id_, name_, display_name_, description) VALUES
(1,'sample_script','Sample Groovy Script','This is a sample Groovy script.');
```

		Ъ	
-	_		
-	_	-1	
		_ I	

**Note** • You need a commit; statement if executing this on Oracle.

## **Running an Electronic Update**

FlexNet Code Insight supports electronic updates of product data in several ways. An update can be applied either automatically on a recurring basis, or manually via the Web UI. In case of a manual update, the FlexNet Code Insight Update HTTPS service is used whereby an update archive is downloaded and processed by the system, or in case of a setup where internet access is not available, a local update archive can be used.

### **Running an Electronic Update Manually**

### 

Task

To run an electronic update manually, do the following:

- 1. Log in to FlexNet Code Insight as Application Administrator.
- **2.** Navigate to the Administration  $\rightarrow$  Updates menu option.

### Using the Electronic Update Server (HTTP)

On the **Last Update** tab, click the **Check for Electronic Update** button to connect to the FlexNet Code Insight Update HTTPS server and check for updates. If one is available, follow the prompts to process the update. The following types of information may be provided in updates:

- New components, versions, licenses, and vulnerabilities
- License by version mappings
- License families
- License detection data
- License obligations data

- License compatibility data
- AutoExpert<sup>™</sup> rules

### Using a Local Electronic Update Archive

# Task

To use a local electronic update archive, do the following:

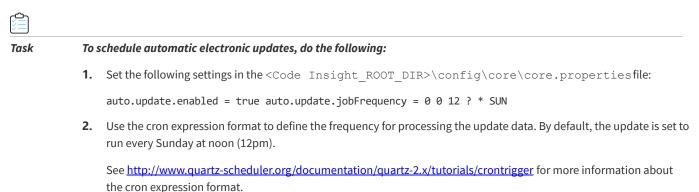
1. Switch to the Manual Update tab.

2	Users
8	Teams
13	Projects
0	Metadata
	Import
F	Scripting
82	Updates

2. Browse for the manifest (update\_manifest.txt) and data file (update.zip). Follow the prompts to process the update.

🚱 Home   🥥 Administration 🔻			Welcome Admin 🛛 🌡 My Settings	🛟 Help   🐗 Logout
Last Update	Manual Update	Update History		
Check for Elec	stronic Update			

### **Scheduling Automatic Electronic Updates**



Viewing Electronic Update History

Select the **Update History** tab to view and sort the number of affected projects and the number of affected inventory items based on data changes via the electronic update.

Last Update	Manual Update	Update History	
Date Process	ed +	Number of Affected Projects	Number of Affected Inventory Items

# **Email Notifications**

FlexNet Code Insight sends email notifications for various events in the application. Email notifications use HTML templates to generate the appropriate email subject line and body text. The email templates can be found in the <CODEINSIGHT\_ROOT\_DIR>\config\core\email\ directory, and they can be modified as necessary.

### **Email Event Triggers and Notifications**

The following table lists events that trigger an email notification, the users who receive the email notification, and whether any configuration option exits for the given event.

#### Table 3-1 • Email Triggers and Notifications

Email Triggering Event	Email Notification To	Configuration Option		
Administrative				
Code Insight license close to expiration	Application administrators	None		
New user account created	New user	None		
Forgot password	Current user	None		
Project				
New project created	Project owner	None		
	Policy administrators			
Project copy completed	Project owner for new project	None		
Project summary per selected frequency	Project owner	Frequency		
Task is reassigned to another user	New task owner	None		
Policy				
Policy created, updated, or deleted	Policy administrators	Which roles get notified		
Electronic Updates				
Update service completed with failed status	Application administrator	None		

#### Table 3-1 • Email Triggers and Notifications

Email Triggering Event	Email Notification To	Configuration Option
Scanning		
Scan server down	Application administrators	None
Scan task completion	User that scheduled tasks	None
Inventory		
Inventory scheduled for full review	First pool of reviewers	None
Inventory with vulnerabilities scheduled for full review	Security Analysts for project	None
Vulnerability alert (inventory item with	Project owner	None
new vulnerabilities)	Security Analysts for project	
Inventory checklist item created, edited, or deleted	User assigned to checklist item	None
Inventory checklist item marked as	Project owner Posted by user	None
completed	Marked complete by user	
Inventory question created, edited, or reassigned with specified assignCode Insight	User assigned to question	None
Inventory question answered or answer updated	Project owner Posted by user Answered by user	None
Requests		
New request submitted	Requester and first review level users	None
Existing request renewed and resubmitted	Requester and first review level users	None
Request field value(s) updated by reviewer	All request participants who have touched request	Which project participants (by role) get notified
Comment added to request	All request participants who have touched request	Which project participants (by role) get notified

#### Table 3-1 • Email Triggers and Notifications

Email Triggering Event	Email Notification To	Configuration Option
Request recalled	All request participants who have touched request	None
Request in pending state for long time	Current actors (requester or reviewer)	Frequency
Request reached terminal state (approved/ rejected)	All request participants who have touched request	None

#### Chapter 3 Application Administrator Tasks

Email Notifications

# **Owner Setup Tasks**

The owner of a project has specific tasks to complete before a project launch. These tasks include the following:

- Configuring and Editing Your Project
- Adding and Deleting Requesters
- Editing, Adding, and Deleting Project Reviewers
- Viewing, Adding, and Deleting Policies
- Viewing Scan Engine Queues
- Generating Reports
- Conducting Research

# **Configuring and Editing Your Project**

General project information contains the following items:

- Name
- Description
- Team
- Advanced Options
- Enable Inventory Quick Review
- Auto-Publish System-Detected Inventory
- Apply Policies to Inventory
- Request Form
- Owner
- Auditor

- Security Analyst
- Workspaces
- Review levels (along with any conditions required to enable them, by default, all review levels are always enabled)

Task

#### To edit, delete, or add information to a project, do as follows:

- 1. Log in to FlexNet Code Insight as an Owner.
- 2. Click Home in the Main menu bar. The Home page appears:

1 My Security Alerts	🌛 My Tasks 🛛 👷 My Sh	ortcuts 🛛 🕰 Dashboard		
Filter: In Progress Pro	jects 💌 Search:		P	
Project +	Audit		Inventory Review	Inventory with Legal / Remediation / Security Issues
ePortal 1.3		indicators reviewed	Rejected: 2   Pending: 2   Approved: 3 Total inventory items: 9 Un-reviewed inventory items: 2	Legal   Open: 2   Completed: 0   None: 7 Remediation   Open: 3   Completed: 0   None: 0 Security Issues   Open: 1   Completed: 0   None
ePortal 1.4		indicators reviewed	Rejected: 2   Pending: 2   Approved: 3 Total inventory items: 9 Un-reviewed inventory items: 2	Legal   Open: 2   Completed: 0   None: 7 Remediation   Open: 3   Completed: 0   None: 1

3. On the top left of the page, click the **My Projects** button to open the **My Projects** page, which lists all projects:

💋 My Projects										
Basic Search Advance	ed Search   Filter	In Progress Proje	cts	Y Search:			Q			
Name			Team		Owner	Status	Inventory	Requests	Tasks	Actions
ePortal 1.3			Engineeri	ing	Owner Smith	In Progress	9	8	6	070
ePortal 1.4			Engineeri	ing	Alex Rybak	In Progress	9	8	0	a

🚳 Home | 💋 My Projects | 🚦 Policies | 🕑 Scheduler | </u> Research | 🔀 Reports Welcome Owner | 🏭 My Settings | 🛟 Help | 🖏 Logout 💋 ePortal 1.3 Summary Workspaces Inventory Requests Tasks Policies Comments Id ePortal 1.3 Name Team Engineering Owner Owner Smith Auditors Alex Rybak, Auditor Smith Security Analysts Alex Rybak Observers Observer Smith, Super User QuickReview Facilitators Alex Rybak, Owner Smith, Super User Advanced Options Enable Inventory Quick Review: Yes Project Summary Emails: Never Auto-Publish Inventory: Yes Request Review Reminder Emails: Never Apply Policies to Inventory: Yes Request Form: Palamida Default Short Request Form Definition Allow Requester to Select First Reviewer: No Project Metadata View Project Metadata Aliased Projects There is no aliased project for this project. Child Projects There are no child projects for this project. Status In Progress ~ Progress [View Project Inventory Snapshots] [Take Project Inventory Snapshot] [Scan Project] Audit 19 of 41 files with indicators reviewed 10 of 38 files without indicators reviewed Inventory Review 9 total (2 rejected, 2 pending review, 3 approved, and 2 not yet reviewed) ery with Legal / Remediation / Security Issues Legal: 9 total (2 open, 0 completed, and 7 none required) Remediation: 9 total (3 open, 0 completed, and 6 none required) Security: 9 total (1 open, 0 completed, and 8 none required)

#### 4. Click the project name. The **Project Summary** page appears:

On the **Summary** tab you can view and scan the project using the buttons in the **Progress** section:

- 5. Click the Back button to return to the My Projects page.
- 6. Click the Pencil and Paper icon to the right of the project you want to edit. The Project Details page appears:

Name		
Description		
Team	Select a team	*

- 7. For each project, you can edit general project information, as well as the lists of users associated with each project:
  - Observers: read-only view of project data
  - QuickReview<sup>™</sup> Facilitators: approve/reject inventory items
  - Auditors: launch Detector to review scan results and conduct audit
  - Security Analysts: review vulnerabilities associated with inventory items
  - **Requesters**: submit request for use of OSS/TP software

- **Reviewers**: review requests
- 8. Enter text in the Name and Description fields.

**Note** • The selected Team is not editable via the Edit Project page. Only an application administrator can change the team to which the project is assigned via the Administrator  $\rightarrow$  Projects  $\rightarrow$  Project Details page.

- 9. Select the Owner and Project Summary Email Frequency using the pull-down menu.
- **10.** Choose the Request Review Reminder email delivery frequencies from the pull-down menu.
- **11.** Select either a long or short request form type via the pull-down menu.
- **12.** (Optional) Check the Advanced Options checkboxes:
  - Enable Inventory Quick Review: allows an Approve/Reject inventory option for the project owner on the Inventory Details page. If either of these options is selected, then the request workflow is not required.
  - Auto-Publish System-Detected Inventory: automatically publishes any system-detected groups from Detector as inventory.
  - Apply Policies to Inventory: applies any always approve/reject policies to published inventory and sets the Review Status to Approved or Rejected if a matching policy exists. All other inventory items receive a Review Status of Ready for Review.
- 13. Add or delete Review Levels and Child Projects in the associated fields if you wish. To add a review level, for example, if you want to differentiate between specific technical review levels in a software development project, click on the Add A Review Level Plus icon. This opens a text field into which you can enter a name of your choosing for the new review level. This also adds a new tab to the Project Details page on which you must select both the appropriate reviewers for a given level, and optionally define the conditions to activate this level if it should not always be active. By default, all review levels are created as enabled, but levels may be changed to conditionally enabled if desired.
- 14. Click Alias Project to search aliased projects.
- 15. To edit the name of a review level, click the Pencil and Paper icon associated with that particular review level.
- 16. To delete a review level, click the X.
- **17.** To add the name of a Child Project, click on the green Plusicon.
- 18. To edit or delete a child project, click on Pencil and Paper icon to edit or the X icon to delete.
- **19.** Select a scan server from the pull-down menu. This feature allows all workspaces to reside on one server.
- 20. To select a Scan Root Path, click Browse, Type, or Remove.
- 21. Click Save to save your work.

# **Adding and Deleting Requesters**

Task

To edit, add, or delete requesters associated with a specific project, do as follows:

- 1. Click the My Projects button in the top left corner.
- 2. Click the Pencil and Paper icon next to the project you want to edit.
- 3. Select the Requesters tab:

a P	roject Details											
Ge	eral Information	Observers	QuickRevier	v Facilitators	Auditors	Security Analysts	Request	ters	Reviewers			
Re	questers							User	Lists			
Sea	roh:		Q		🔕 Delete F	lequesters 🗿 Add R	equesters	Search	ho	٩	🙆 Delete	O Add
0	First Name +	Last Na	ime	Email				U	ser List Name 🔺			
m	Alex	Rybak		arybak@pi	alamida.com							
É)	Requester1	One		user@ema	il.com							
en l	Requester2	Two		user@ema	il.com							
23	Requester3	Three		user@ema	il.com							
0	Requester4	Four		user@ema	il.com							
2	Requester5	Five		user@ema	il.com							
1	Requester6	Six		user@ema	il.com							
	Requester7	Seven		user@ema	il.com							
	Requester8	Eight		user@ema	il.com							
m	Requester9	Nine		user@ema	il.com							
14	I Page 1	of t   P Pl	50 Show	41			- 10 of 10	14 4	Pane 1 o	f1  ≥ ≥  😤   Sh	All All	

- 4. To delete a requester, select the name you want to delete and click **Delete Requesters**.
- 5. Add a requester in one of the following ways (a or b):
  - a. Click the green Add Requester button in the left pane. The Add Requester dialog box opens with names of possible requesters.

	arch:		P	Selected Requ	esters
m	First Name 🔺	Last Name	Email	First Name +	Last Name
P1	Super	User	user@email.com		

- Select the name of the requester you want to add. The name appears in the **Selected Requester** list to the right of the name.
- Click **Add** to add this person to the project in the role of a requester.
- **b.** Click **Add Requestor from User List** or a user list name in the **Search** field. A dialog box opens from which you can choose a specific user list. You can create user lists that filter users by project roles.

# Editing, Adding, and Deleting Project Reviewers

Task

To edit, add, or delete reviewers associated with a specific project, do the following:

- 1. Click My Projects in the top left corner.
- 2. Click the Pencil and Paper icon next to the project you want to edit. The Project Details page opens.
- 3. Select the Reviewers tab:

Project Details											
General Information	Observers	QuickReview	v Facilitators	Auditors	Security Analysts	Requeste	ers	Reviewers			
Reviewers							Use	r Lists			
Search:		P		🙆 Delete	Reviewers 🗿 Add	Reviewers	Sear	roh:	Q	🔕 Delete	O Add
First Name +	Last Na	ame	Email				0	User List Name +			
Alex	Rybak		arybak@p	alamida.com	1						
Reviewer1	One		user@ema	iil.com							
Reviewer2	Two		user@ema	iil.com							
Reviewer3	Three		user@ema	il.com							
Reviewer4	Four		user@ema	il.com							
Reviewer5	Five		user@ema	il.com							
Reviewer6	Six		user@ema	il.com							
Reviewer7	Seven		user@ema	il.com							
Reviewer8	Eight		user@ema	il.com							
Reviewer9	Nine		user@ema	il.com							
N 4 Page 1	of 1 > >	Show	AR			1 - 10 of 10	14	R Page 1 o	1   > >   2   5	Show All	

- 4. Add or delete a reviewer:
  - To delete a reviewer, select the name you want to delete, and click **Delete Reviewer**.
  - To add a reviewer, click **Add Reviewer** and select the name of the reviewer you want to add from the **Reviewers** dialog:

Search:			0	Selected Revie	ewers
Firs	st Name +	Last Name	Email	First Name +	Last Name
E Sup	er	User	user@email.com		
0.0	2000				
24 C.M.	Page	1 of 1	æ 1-1o	07 1	

The name appears in the **Selected Reviewers** list box.

5. Click at the bottom of the box to add this person to the project in the role of a reviewer.

# Viewing, Adding, and Deleting Policies

Policies are used by FlexNet Code Insight to automate the review of inventory items (in a QuickReview<sup>™</sup> scenario) or requests to use OSS components (in a full review scenario). Policies can be defined up-front and re- evaluated each time a new project is created. Policies can also be built off of requests that are being reviewed by someone with the policy administrator permission. Creating a policy during the time of request review will result in a very specific policy at the current project scope and will automate the action taken by the reviewer at the time of the policy creation. The purpose of policies is two-fold:

- Policy notifications (flags in the web UI and Detector auditing client) inform the user whether the component and/or license has an associated policy. This information may be used to increase the priority of reviewing particular items in cases where the associated components and/or licenses have an auto-reject policy.
- Policies are also used to automate manual reviews in cases where a particular component or licenses has previously been reviewed and future manual reviews are no longernecessary.

Anyone with policy administrator permissions can create, add, delete, and edit policies. The system administrator allows any user to have these permissions by checking Policy Administrator in the role box when setting up or editing a new user.

### **Viewing and Editing Policies**

🛅 Task

#### To view or edit policies, do the following:

- 1. Log in as policy administrator or make sure your administrator checked the role of **Policy Admin** in your **User Details**.
- 2. Click Policies on the Main menu bar. The Policies page appears:

P P	olicies						
Basi	c Search Advanced Search   Sear	ch:		٩		O Add	New Polic
Id	Name +	Scope	Action	Component	License	Last Updated	Acti
1	GPLv2 Not Allowed	Global	Reject	Any Component (Any Version)	GNU General Public License v2.0	08/03/2011	20
4	LGPL v2.1 Allowed No Mods	Global	Approve	Any Component (Any Version)	GNU Lesser General Public License v2.1	03/27/2012	20
2	zlib 1.2.2 Not Allowed	Global	Reject	zlib (1.2.2)	Any License	08/03/2011	20

3. View or edit policies by clicking the Pencil and Paper icon associated with an existing policy.

Ŷ

## Adding a Policy

#### Task add a policy, do the following:

1. Click Add New Policy on the right side of the page to create a new policy. The General Information and Attributes tab opens.

Policy Details	
General Information	plicy Attributes
Name	
Description	
<ul><li>Action</li><li>Component Name</li></ul>	Search Component Any Component Versions View Component Metadets
Scope	🔽 Global
Attachments	Browse Uplosd
Conditions of Use	Add Condition of Use
Policy Metadata	Create Policy Metadata

- 2. On the General Information tab, select Approve, Reject, or Manual Review from the Action pull-down menu.
- **3.** Determine the scope. Global is the default. Uncheck the Global checkbox if you want to apply the policy to a specific team. Select the appropriate team by double-clicking on the name of the team in the left column, thereby moving it to the right column.
- 4. Add an attachment if necessary.
- 5. Click Add Condition of Use. The Add Conditions of Use dialog appears:

Condition of Use:	
Required:	(Required conditions must be acknowledged by requester)

- 6. Enter text explaining specific conditions of use for this policy.
- 7. Check the Required checkbox if you want the requester to be required to acknowledge the policy conditions of use.
- 8. Click Save to save your work.
- 9. Select the Policy Attributes tab.

- **10.** Select a Request Form using the pull-down menu to inform the system as to which request form attributes to load. (You must select a request form type to set policy attributes.)
- 11. Click the Add/Remove Policy Attribute button. The Policy Attribute checkbox opens.

Policy Attributes	×
Usage Modifications Encryption Vault	
Select the intended usage of the requested component:	
Does the requested component replace another component or any proprietary or 3rd-party code?	
Explain in detail:	
Select how the requested component will be linked to the product or service:	
Explain in detail:	
Save Cancel	

Any boxes you check on the **Usage**, **Modifications**, **Encryption**, and **Vault** tabs become part of the viewable policy attributes. When you click **Save**, the **Policy Attribute** tab is populated with those checked boxes.:

🚱 Home   🤪 My Projects   🚦 Policies   😏 Research	Welcome Policy	🔒 🏭 My Settings	🛟 Help	🖏 Logo
Policy Details				
General Information Policy Attributes				
Select request form from which to show policy attributes:				
×				
Select the intended usage of the requested component:				
Explain in detail:           Select how the requested component will be linked to the product or service:				
Explain in detail:				
Add/Remove Policy Attribute	es			
Save Cancel				

### Note about Policy Conflicts

FlexNet Code Insight does not support conflict resolution in cases where multiple policies apply to a given inventory item or request. There are conflicting policy validations in place to ensure that more than one identical policy is not created with alternate actions. However, policies of various specificities can be defined and more than one can apply at a given time. In such a scenario, the policy that was defined first (by creation date/time) will take precedence. Below is an example:

- Policy #1 Automatically approve component: Mozilla Firefox
- Policy #2 Manually review license: Mozilla Public License (MPL), Version 1.1

If an inventory item with Mozilla Firefox under the Mozilla Public License (MPL), Version 1.1 is evaluated by policies, the first policy will take precedence, since it was created before the second policy, and the inventory item would be automatically-approved.

### Copying a Policy to Create a New Policy

Instead of creating a new policy from scratch, you can copy and modify an existing policy.

Task	To copy and modify an existing policy, do the following:

- 1. Select an existing policy, and then click the Copy Policy icon (). The copied policy appears in the **Policy Details** window.
- 2. To create a new policy from the copy, modify the copied policy and save it as a new policy.

# **Viewing Scan Engine Queues**

To view the Scan Engine task queue and task history for a workspace scan server, log in as someone other than an admin or a policy admin, and do as follows:

# Task

To view the scan engine queue, do the following:

1. Click Scheduler on the Main menu bar. The Scheduler page appears with Task Queue and Task History tabs.

Welcome Owner   🏭 My Settings 🛛 🥇 Hel	p   🍕 Logou
	Welcome Owner   🌺 My Settings 😽 Hel

- 2. Select a server from the Scan Server pull-down menu, and you can view the progression of the task queue and the task history associated with that server.
- 3. Click **Refresh Page** to see the latest active and pending tasks.

4. Select the **Task History** tab to view a list of tasks and dates. To sort the columns in ascending or descending order, click the **Task Status** column heading or any other column heading:

Scheduler					
Scan Server: server1	×				
Task Queue Task I	History				
Filter: All Completed Ta	sks 💌				
Workspace	Project	Task Started	Task Completed +	Task Type	Task Status
ePortal_1-3	ePortal 1.3	01/05/2012 10:08	01/05/2012 10:14	Report - File Evidence Map Report	Completed
ePortal_1-3	ePortal 1.3	01/05/2012 10:03	01/05/2012 10:08	Scan	Completed
ePortal_1-3	ePortal 1.3	12/01/2011 10:28	12/01/2011 10:33	Report - File Evidence Map Report	Completed
ePortal_1-3	ePortal 1.3	12/01/2011 10:28	12/01/2011 10:28	Report - Third-Party Indicators Report	Completed
ePortal_1-3	ePortal 1.3	12/01/2011 10:28	12/01/2011 10:28	Report - Scanned Files Report	Completed
eronal_1-3					

## **Generating Reports**

You can generate many types of reports. To see available report types, click the **Reports** button on the **Main** menu bar.

- Reports are defined in the database. Refer to the default\_reports.sqlscript for a sample definition of the default reports.
- Reports are generated on the server using a groovy script for the report logic and velocity templates for the rendering logic. You can modify both of these sets of files. Your modifications will influence the report the next time it is generated.
- Generated reports *do not* remain on the server. They are deleted once either the current user's session times out or is closed out.
- FlexNet Code Insight offers a Third-Party Notices report as well as the FlexNet Code Insight report, which is an extensive project detail summary report.

### **Generating a Project Details Report**

### 🚰 Task

#### To generate a project details report, do as follows:

1. Click **Reports** on the **Main** menu bar. The **Reports** page appears:

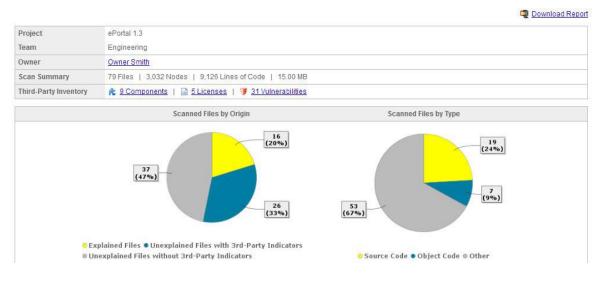
Re	ports
Palam	ida Report
Contai	ins full project summary including scan details, component and license inventory, and vulnerability details.
Projec	t Details Report
	nts all project details in a single report suitable for project status and final project documentation and sign-off. It includes project inventory, project requests, and project ta comprehensive information for each item, task and request.
Projec	st Inventory Delta Report
Conta	ins a delta between the project inventory at 2 selected times. To be used to compare the state of a single project at two different times or across 2 projects.
Audit	Report
Provid	tes a detailed summary of all detected inventory along with auditor comments and file appendices
Compo	onent Usage Report
	des summary of component reuse across multiple projects. For each component used, a summary of its use in each project is provided, including version details, licensing nation, vulnerability data, and associated request details.
Licens	se Usage Report
	arizes license usage across multiple projects. The information is presented a list of Licenses, along with their details, and a list of the components in the projects that are ed under the license.
Policy	Report
Provid	tes a detailed summary of all Policies applicable within the selected scope.
Invent	tory Report
Compr	rehensive listing of all items in the selected projects, including licensing information, available versions, vulnerability data, and associated request details.
Third-	Party Notices Report
Palam	ida standard third-party notices report.
Scann	ned Files Review Progress Report
Summ	ary of review status of scanned files across all workspaces in selected projects.
Licens	se Obligations Report
Provid	les a summary of License Obligations corresponding to items found in inventory.

2. Select the FlexNet Code Insight Report link. The FlexNet Code Insight Report page appears:

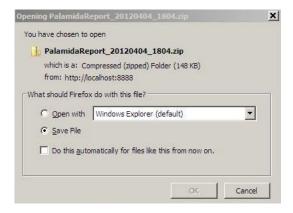
Report Name	Palamida Report	
Report Description	Contains full project summary including scan details, component and license inventory, and vulnerability details.	
Report Scope	Global	
	Teams	
	Engineering	
	-	
	Projects	
	ePortal 1.3	
	ePortal 1.4	
Include Scanned Files in Report? (This option will make report run longer)		
Show Inventory File Details?		
(This option will make report run longer)		

3. You can enter or edit a report name and description on this page.

- 4. Uncheck the Global checkbox.
- 5. Select a team name in the **Teams** column to enable and view associated project choices in the **Project** pane.
- 6. Select the project in the Projects column.
- 7. Click Generate to create the report. When the report is ready to view, a box opens with a link to view the report.
- 8. Click the report link and the report opens:



9. Click the **Download Report** link to download the report as a compressed file in the default **Report** directory:



**10.** To view a specific aspect of the project report, click one of the links in the **Third-Party Inventory** section. For example, click on the **Licenses** link. Reports contain a variety of graphical representations and detailed information:

Project		ePortal 1.3									
Team		Engineering									
Third-Pa	arty Inventory	R 9 Components   🗟 5 Licenses	🔰 <u>31 Vulnerabilities</u>								
			Com	ponents Instances	s by License						
Legend	I										
L2: GNU L3: MIT L4: scri	U Affero Genera U General Publi license (also X ptaculous 1.8.1 filopno License	11) License		Component Instances	1 J	ا ع conses (se	1 I I I I I I I I I I I I I I I I I I I	5 1 5 for details)			
#	License		Usage								
1	GNU Affero G	eneral Public License v3.0	Component	Component		Encryption	Vulnerabilities	Files	Status		
		itext (5.1.2)	itext (5.1.2)					1	Pending Review		
2 GNU General Public License v3.0		Component	Component			Encryption	Vulnerabilities	Files	Status		
			mcrvpt (2.6.8)							1	Ready for Review
3	MIT license (a	Iso X11)	Component					Encryption	Vulnerabilities	Files	Status
			prototype (1.6.0.2)							1	Approved

### **Generating Inventory Reports**

# Task

To generate an Inventory report, do the following:

- 1. Click Reports on the Main menu bar. The Reports page appears.
- 2. Select the Inventory Report link. The Inventory Report page appears:

Report Name	Inventory Report
Report Description	Comprehensive listing of all items in the selected projects, including licensing information, available versions, vulnerability data, and associated request details.
Report Scope	Global Teams
	Engineering
	Projects
	ePortal 1.3 ePortal 1.4
Show Only Items with Encryption	
Show Only Items with Vulnerabilities	
Generate Excel Version	
Generate XML Version	<b>v</b>

- 3. You can enter or edit a report name and description on this page.
- 4. You must select a team name in the Teams column to enable and view associated project choices in the Project pane.
- 5. Click the **Global** checkbox or double-click on a team in the **Teams** column to view associated projects in the Projects pane. Then, select the project in the Projects column.

- 6. To create versions of the report in Excel or XML format, check the associated checkboxes.
- 7. Click **Generate**. When the **Inventory Report** is available for viewing, a dialog box opens with a link to the report. The report is presented for the project you selected. Each **Inventory** report has two sections. The **Summary** section provides general project information. The **Inventory** section lists ID, name, component, description, license, review status, encryption, and vulnerabilities. Each element in the report is linked to information:

entory Re	port					riteanesual, np	ril 4, 2012 at 6:1
Project Sum	mary						
Project	ePortal 1.3	3					
eam	Engineeri	ng					
Owner	Owner Sm	nith (415-555-1212	)				
Auditors Security Analys	and the second s	nith (415-555-1212	3)				
Observers		Smith (415-555-12 er (415-555-1212)	12)				
ld	Name	Component	Description	License	Review Status	Encryption	1.
ld 4	Name zlib 1.2.2	Component zlib (1.2.2)	Description zlib is designed to be a free, general-purpose, legally unencumbered that is, not covered by any patents	License zlib/libpng License	Review Status	Encryption	Vulnerabilitie Yes (2)
			<ul> <li>lossless data-compression library for use on virtually any computer hardware and operating system.</li> <li>The zlib data format is itself portable across platforms.</li> </ul>				
2025	mcrypt 2.6.8	mcrypt (2.6.8)	mcrypt, and the accompanying libmcrypt, are intended to be replacements for the old Unix crypt, except that they are under the GPL and support an ever-wider range of algorithms and modes.	GNU General Public License v3.0	Ready for Review		
5         prototype 1.6.0.2         prototype (1.6.0.2)         Prototype is a JavaScript Framework that aims to ease development of dynamic web applications. Featuring a unique, easy-to-use tookit for class-driven development and the nicest / jaxi library around, Prototype is guidy becoming the codebase of choice for web application developers everywhere         MIT license (also X11)         Approved           5         Prototype is guidy becoming the codebase of choice for web application developers everywhere         X11)         X11         X11		Approved	8	1921			
2			<u>Yes (1)</u>				
9	IText 5.1.2	itext (5.1.2)	ITextÃ,®, a JAVA-PDF library	GNU Affero General Public License v3.0	Pending Review (Waiting for	-	1.00

## **Conducting Research**

The Research feature allows you to search the FlexNet Code Insight Data Library for components and licenses, as well as to create and delete components, component versions, licenses, and vulnerabilities (provided that you have the correct permissions).



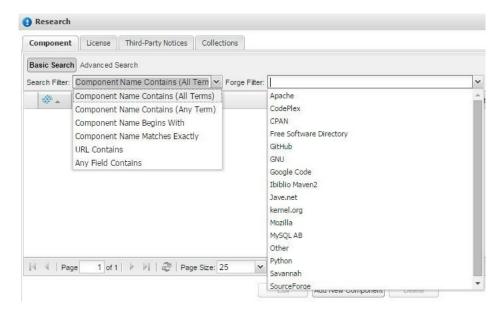
Note • Only custom data may be deleted.

### Searching for Components

### Task

To search for a component in the FlexNet Code Insight Data Library, do the following:

1. Click **Research** on the **Main** menu bar. The **Research** page appears:



The default for component search is a **Basic Search**. It includes a Search Filter and Forge Filter to help you limit your search results.

**Note** • The defaults for these filters are configured by the FlexNet Code Insight Administrator and may be edited at any time.

- 2. Select a search filter from the pull-down menu:
  - Component Name Contains (All Terms): searches all component names and returns all components whose name contains *all* of the submitted search terms. Note: Component Name refers to the name of the component assigned by FlexNet Code Insight or by the user in the case of a custom component. Component Names typically do not contain spaces.
  - Component Name Contains (Any Terms): searches component names and returns all components in which the component name contains any of the submitted search terms.
  - **Component Name Begins With**: searches component names and returns all components in which the component name *begins with* a submitted search term.
  - **Component Name Matches Exactly**: searches component names and returns all components whose name matches the submitted search term exactly.
  - URL Contains: searches component URLs and returns all components whose URL matches the submitted search term URL in part or in full.
  - Any Field Contains: searches all the fields outlined above, as well as the component Description field, and returns all components that contain text in one of these fields that matches the submitted search term.

- 3. Select a forge from the Forge Filter or leave it blank to search across all forges. The Forge Filter allows you to limit your search to a specific forge, also known as a "repository" or "source" of code. For example, the Free Software Directory forge references all components in the FlexNet Code Insight Data Library that were obtained from <a href="https://directory.fsf.org">https://directory.fsf.org</a>, and the GitHub forge references all projects obtained from <a href="https://directory.fsf.org">https://directory.fsf.org</a>, and the GitHub forge references all projects obtained from <a href="https://directory.fsf.org">https://directory.fsf.org</a>.
- 4. Enter the name of a component in the **Search For** box and click the **Search** button (<sup>Search</sup>) to search for the component. Every component that matches the specified search criteria will be listed in the results. For example, a search for the term "openssl" without a specified forge filter, results in multiple entries for the OpenSSL component, including an entry for the component obtained from "The Free Software Foundation", an entry from the "OpenSSL Project" website (forge is listed as "Other") and an entry for the component obtained from "GitHub".

arch Advanced Search							
Advanced Search							(?) Help
er: Component Name Con	tains (All Tern 🔽 Forge Filter:			Search For:	openssl		🖉 🔑 Search
Name	Description	Forge	Encryption	Vulnerabilities	Policy	Review History	Custom
openssi	The OpenSSL Project is a collaborative effort t.	Free Software Directory	9	<b>(</b>	$h_0$		-
openssi	The OpenSSL Project is a collaborative effort t.	Other	8		1º		
openssl-openssl	openssi's openssi at github.com	GitHub	9		1º		
allwinnerwk-platform_ex	allwinnerwk's platform_external_openssI at gith	GitHub			Ju.		
android-area51-external	android-area51's external_openssI at github.cc	GitHub			10		
android-platform_extern	android's platform_external_openssl at github.c	GitHub			10		
aosm-openssi096	aosm's openssi096 at github.com	GitHub			Ju .		
Page 1 of 7 🕨 🕅	₽ Page Size: 25 💌						1 - 25 of 15
	Name openssI openssI openssI-openssI allwinnerwk-platform_ex android-area51-external android-platform_extern aosm-openssI096	openssi         The OpenSSL Project is a collaborative effort t.           openssi         The OpenSSL Project is a collaborative effort t.           openssi-openssi         openssi's openssi at github.com           allwinnerwk-platform_ex         allwinnerwk's platform_external_openssi at github.co           android-areaS1-external         android's platform_external_openssi at github.co           android-platform_extern         android's platform_external_openssi at github.co           aosm-openssi096         aosm's openssi096 at github.com	Name         Description         Forge           openssl         The OpenSSL Project is a collaborative effort t. Free Software Directory           openssl         The OpenSSL Project is a collaborative effort t. Other           openssl-openssl         openssl's openssl at github.com         GitHub           allwinnerwk-platform_ex         allwinnerwk's platform_external_openssl at gith ditHub         GitHub           android-area51-external         android's platform_external_openssl at github.c GitHub         GitHub           android-platform_extern         android's platform_external_openssl at github.c GitHub         GitHub	Name         Description         Forge         Encryption           openss1         The OpenSSL Project is a collaborative effort t. Free Software Directory         Image: Collaborative effort t. Free Software Directory         Image: Collaborative effort t. Other         Image: Collaborative effort t. Other	Name         Description         Forge         Encryption         Vulnerabilities           openss1         The OpenSSL Project is a collaborative effort t. Free Software Directory         Image: Collaborative effort t. Other         Image: C	Name     Description     Forge     Encryption     Vulnerabilities     Policy       openss1     The OpenSSL Project is a collaborative effort t. Free Software Directory     Image: Collaborative effort t. Free Software Directory     Image: Collaborative effort t. Other     Imag	Name     Description     Forge     Encryption     Vulnerabilities     Policy     Review History       openss1     The OpenSSL Project is a collaborative effort I. Free Software Directory     Image: Collaborative effort I. Other     Image: Collaborative effort I. Other

The result set is sorted first by all components marked as *Important*, indicated by the  $\stackrel{\text{def}}{=}$  icon to the left of the component name. A component is designated *Important* if it meets one or more of the following criteria:

- FlexNet Code Insight Top Component: this popular OSS component was manually inspected and edited by the FlexNet Code Insight Library Team for accuracy. Information for FlexNet Code Insight Top Components is delivered to the system via Electronic Update. Ensure that you have the latest update for the most accurate information.
- **Referenced Component**: the component is associated with a Request (including Draft and Rejected request), Policy, Group (including unpublished group), Inventory Item or third-party notice. These components are classified as Important because they are currently in use by one or more FlexNet Code Insight users.
- **Custom Component:** the component was manually created by a FlexNet Code Insight user and marked as Important via the Important checkbox in Component Details. Note: custom components have negative component IDs. A custom component can be unmarked as Important by unchecking the Important checkbox in the Edit Component menu.
- 5. To re-sort the result set, select any column to merge the results for Important and all other components into a single list.
- 6. Click expand (±) to the left of the component entry to expand to view component details such as Title, Forge, URL, Description, Versions, Licenses, Vulnerabilities, Encryption information and Custom information.
- 7. Click one of the **Manage** buttons to view detailed information for Versions, Licenses and other data available for the component entry.

The following list summarizes other features that may be available in **Component Details**.

Component	lcon	Description
Encryption Details	9	Details related to whether or not encryption is required.
Security Vulnerability Details icon	Ø	Vulnerabilities associated with a specific version.
Component Policy Flag icons	۳	Component always approved for use.
	۳	Component always rejected for uses.
	۳	Component has unknown policy since it depends on use.
	h	Component does not have a matching policy.
Approval Status icons	0	Component has been previously Approved.
	٥	Component has been previously Rejected.

### **Component Search Tips**

The following are some tips to maximize your success when searching:

- To get more results, use one of the **Component Name Contains** search filters and substitute spaces for dashes.
- Use the **URL Contains** search filter to search for the URL. For better results, use only essential elements of the URL. For example, if the URL is <u>https://www.github.com/facebook/facebook-ios-sdk</u> try searching with just github.com/facebook/facebook-ios-sdk, or for more results, try github.com/facebook/.
- To narrow the search, click the Advanced Search tab. The Edit Component Search Criteria dialog appears:

basic bearch			Saved Component Se	arches 🜔 Add New	Component Search	(🕑 Help	
- #	Name		Description Forge Encryption Vulnera				
Ŧ	New Component	Search	Edit Componen				
Ð	Name		* Entity	License			~
	Description		* Field	Name			~
			* Operator	contains			~
			* Value				Long to
	* Criteria		* value	openssl			

• Add a new component search; try searching based on the component license or other important field. Consult the Advanced Search section for more information on how to configure and use the feature.

### **Component Fields**

The following fields are available for every component in the FlexNet Code Insight system. Additional component data may be stored in custom metadata fields. See Metadata Framework for more information.

Field	Description
Id	The unique ID of the component. Custom components have negative IDs while non- custom have positive IDs.
Name	The name of the component as stored in FlexNet Code Insight.
	FlexNet Code Insight components (non-custom) are typically named according to convention based on the forge from which they are obtained. For example, FlexNet Code Insight components obtained from GitHub include the author name and project name separated by a "-" in the name (OpenSSL from GitHub has the name "openssl- openssl" in FlexNet Code Insight). FlexNet Code Insight component names do not contain spaces.
	Click the <b>Help</b> icon ( () Help ) in the <b>Components Details</b> tab to see other naming conventions based on forge.
Title	The unique title of the component as stored in FlexNet Code Insight, the components ((non-custom)) of which are also named according to the convention based on the forge. For example, FlexNet Code Insight components obtained from GitHub include the author name and project name separated by a "/" and appended with the term "GitHub" (OpenSSL form GitHub has the title "openssl/openssl – GitHub".
Forge	The downloaded-from URL pointing to the page from which the component was downloaded.
URL	The project URL pointing to the project home page.
Description	The project description.
Encryption	Indicates whether the component uses encryption.
Vulnerabilities	Indicates whether the component contains one or more vulnerable versions.
Custom	Specifies whether the component is custom (user-created) or non- custom (FlexNet Code Insight-created).
Important	Specifies whether the component has been marked for importance by FlexNet Code Insight or is referenced in the system.
Available Platforms	The list of operating systems for which this component is developed (if any).
Categories	The list of tags to classify the component in a catalog-type structure. For example, a user may choose to label a set of components as "Permissive" based on their license type.

#### Table 4-1 • Fields and Descriptions

#### **Table 4-1** • Fields and Descriptions

Field	Description
CPE Name	The list of CPE names from the National Vulnerability Database that are mapped to the component. CPE is a structured naming scheme for information technology system,
Programming Language	The list of programming languages that are used in the codebase for the component.
Last Update Date	The date the codebase was last uploaded to the forge for this component.
Registered Date	The date corresponding to the first code upload to the forge for this component.
Versions	The versions associated with this component.
Licenses	The licenses associated with this component.

### **Component Search FAQ**

#### 1. How can I tell which component is the correct one?

It is always recommended to have some familiarity with the component you are requesting in order to be able to correctly identify it online and in the FlexNet Code Insight Data Library. The URL is a key to identifying components. If it matches the component you are requesting, this is a reliable indicator that they are the same.

If you or the developer downloaded the package from another URL, look up the component online to verify what the canonical project page is. Often, developers will download a package from a site other than the main project page.

Do some Web searches to see if the URLs are related (e.g. fsf.org is related to gnu.org). Look at other information including the descriptions. Look at the project websites and see if they are the same project. If they are, then you can use that component.

#### 2. What if I cannot find the component?

There are several reasons you may not be able to find the component in the FlexNet Code Insight Data Library, for example:

- The component is under a different name in our database. Try to search for the component using some of the techniques above.
- It is a Commercial component.
- The component is considered to be a subcomponent of a larger project. For example, *netkit-base*, *netkit-ftp*, *netkit-rsh*, are all part of *netkit*.
- The component has not been collected into our database. Typical reasons for this include:
- It is not traditionally seen as a software library, but is considered to be a module within a larger work.
- It is no longer available on the Internet.
- It is from a non-electronic source (magazine, book, etc.).
- The component is very new, and has not been collected yet. In this case, you may wish to request the FlexNet Code Insight Library team to collect the component, so the scanner can index the component releases.

• If you cannot find a component in the database, or you wish to categorize them in a different way from how they are in the database, you can create a custom component.

### **Creating a New Component**

Follow these steps to create a new custom component in the FlexNet Code Insight system. To limit the number of duplicates, ensure that you create new components only in the case where you are unable to find the component in the system.

## Task

#### To create a new custom component, do the following:

- 1. Click Research on the Main menu bar. The Research page appears.
- Click Add New Component, and then click Yes when prompted to create the component. The New Component dialog appears:

ew Component		×
General Information	n	
* Name		· · · · · · · · · · · · · · · · · · ·
* Title		
* URL		
* Description		
Forge		~
Encryption	This component contains encryption technology.	-

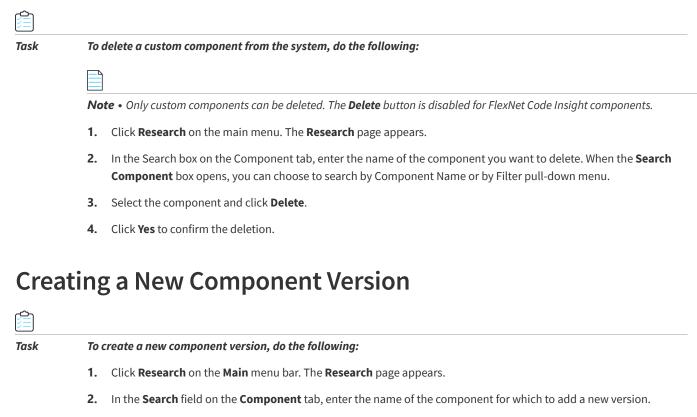
**3.** Enter information in the required fields, which are marked with an asterisk (\*). The remaining fields are optional. See **Component Fields** for more information.

The combination of Name and Title must be unique. For example, if there is already a component name "foo" in the FlexNet Code Insight system, you can create another component named "foo" only if the titles of the two components are not identical.

4. Click **Save** to save the new component. An ID is automatically assigned to the component upon creation. Custom components have negative IDs in the system and are labeled with a **Yes** in the **Custom** field.

### **Deleting a Custom Component**

You can delete only custom components. The Delete feature is disabled for FlexNet Code Insight components. Follow these instructions to delete a custom component from the system.



- 3. Click the magnifying glass.
- 4. Click the left-side **Plus** icon to expand the information about the desired component.
- 5. Click Manage Versions and Vulnerabilities. The Version Details dialog appears.
- 6. Click Add New Version. The Input dialog appears.

Input			×
2	Please enter the	new version name	:
		Cancel	

7. Enter the new component version name and click **OK t**o save the new component version.

### **Deleting a Custom Component Version**

If you create a new component version and decide that you no longer want this component version to be part of the data library, you can delete the component version.

	.	
	.	
	.	
	1	
	Ξ	Ξ

Task

To delete the component version, do the following:

- 1. Click Research on the Main menu bar. The Research page appears.
- 2. In the **Search** field, enter the name of the custom component version you wish todelete.

- 3. Select the name of the component, and then click Delete. The Confirmation dialogappears.
- Click Yes in the Confirmation dialog. 4.

### Adding a New Vulnerability to a Component Version

You can add a vulnerability to the Component Version.

Task	То	create a new v	ulnerability for a component versior	n, do the following:	
	1.	Click <b>Researc</b>	<b>ch</b> on the <b>Main</b> menu bar. The <b>Resea</b> i	<b>rch</b> page appears.	
	2.	In the Search	<b>1</b> field, enter the name of the compon	ent for which you wish to ad	d anew vulnerability.
	3.	Click the <b>ma</b>	gnifying glass.		
	4.	In the search	results, click the left-side <b>Plus</b> icons	to expand the information at	oout the desired component.
	5.	Click Manage	e Versions and Vulnerabilities to ope	en the <b>Version Details</b> dialog	
	6.	Click the <b>shie</b>	eld icon in the Vulnerabilities colum	۱.	
	4. 5.	Click <b>Add Ne</b>	w Vulnerability. The New Vulnerabi	lity dialog appears:	
		New Vulnerabilit	ty for jboss unknown	(	×
		Name			
		Description			
		URL	http://		
		Severity		¥	

8. Enter the required vulnerability name and description, and select a severity from the Severity pull-down menu. The URL field is optional and may be left blank.

9. Click Save to save the new vulnerability and associate it with the selected component version.

Cancel

Save

### **Deleting a Custom Vulnerability**

If you create a new custom vulnerability and decide that you no longer want that vulnerability to be part of the data library, delete the vulnerability by doing as follows.



Note • The following process works only with previously created custom vulnerabilities.

# Task

#### To delete a custom vulnerability, do the following:

- 1. Click Research on the Main menu bar. The Research page appears.
- 2. In the Search box, enter the name of the component for which you wish to delete a new vulnerability.
- 3. Click the Magnifying Glass Search button.
- 4. In the search results, click on the Plus icon to expand the information about the desired component.
- 5. Click Manage Versions and Vulnerabilities. The Version Details dialog appears.
- **6.** Click the red Delete icon next to the custom vulnerability you want to delete. Custom vulnerabilities are only visible if you have previously created them.
- 7. Click Yes to confirm the deletion.

### **Searching for Licenses**



Note • This process works only with previously created custom vulnerabilities.

[	
	Task

#### To see what components are available for a project:

- 1. Click Research on the Main menu Bar. The Research page appears.
- 2. Select the Licenses tab.
- **3.** Enter the name of a license in the Search box, and click the Magnifying glass Search button. Each license that matches the search string appears in the search results with license name, family, policy, and custom information.

Bas	sic Search Advanced	Search   Filter: License Name Begins With	✓ Se	arch: M	π	×P	<	Add New Lic	ens
	Name 🔺				Family		Policy	Custom	
Ξ	MIT license (also X11)						}#1		
	Id	7							1
	Name	MIT license (also X11)							1
	Family	Family							1
	URL	http://spdx.org/licenses/MIT 🚱	http://spdx.org/licenses/MIT 🚱						
	Description	MIT license (also X11)	MIT license (also X11)						
	Category								
	Policy	hu							
	Custom License?	No							
	Family License?	No							
	More Information	View Text View Analysis View Me	tadata View O	bligations	View Comments				

- 4. To refine your search, use the **Filter** pull-down menu. Using the **Any Field Contains** filter value will extend the license search to any associated metadata fields as well.
- 5. Click on the license you want to view.
- **6.** Click on the left-side Plus icons to expand the information about the desired license, as shown in Figure 53. If you click on any of the rows, the Edit button toggles on, and you can edit information.
- **7.** You can now view all license text, analysis, metadata, obligations, and comments associated with this license from this page. (Also, the edit button at the bottom of the window is now enabled.)

### **Editing a License**

# Task

To edit a license, do the following:

- 1. Click **Research** in the Main menu bar.
- 2. Enter a license name in the Search field, and click the Magnifying Glass.
- 3. In the search results, click the Plus icon next to the license you want to edit.
- 4. Click Edit. The Edit License page appears:

General Infor	mation License Analysis License Metadata License Obligations License Comments	
Name	Apache License, Version 2.0	
URL	http://www.apache.org/licenses/LICENSE-2.0.txt	
Description	Apache License, Version 2.0	
Text	Apache License Version 2.0, January 2004 http://www.apache.org/licenses/	
	TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION	
	1. Definitions.	
	"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.	
	"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.	-
Category		~
Is Family?	Yes 💌	
Policy	This license does not have a policy.	

- 5. Click the appropriate tab to view and edit license information:
  - General Information: Name, URL, Description, Text. The Category field, for example, can be set so that you skip legal review. You can also choose to alter the workflow routing if you decide you wish to skip review levels The Family pull-down allows you to indicate if a license is in a family. The Select Family pull-down menu allows you associate the license with a family and choose what characteristics the license will inherit. Policy field contains relevant policy information.
  - License Analysis: This is not editable. Instead you can view the ranking of risk level, license requirements, and descriptions associated with the selected license.

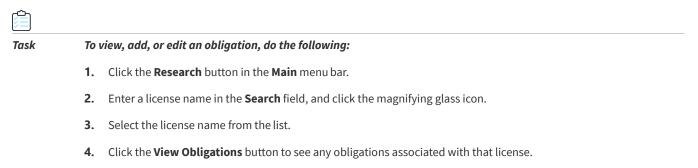
- License Metadata: The license metadata field definitions and value assignments are supported via API and external scripts. The assigned license metadata value fields are visible and can be searched against in the Web UI. see "Metadata Framework" for more information related to the metadata process and supported entities and datatypes.
- License compatibility: On the Metadata tab, at the top, analyses of different license compatibility are provided. These analyses allow you to see which categories of compatibility a license may evoke.
- License Obligations: This tab contains the set of license obligations associated with a given license. If a license belongs to the license family and does not have any license obligations, it will inherit the license obligations from the associated license family. License obligations can be defined in the Web UI by clicking on the Plus icon, or they can be bulk loaded by selecting **Import** from the **Administration** menu. Only an Application Administrator can bulk-import license obligations.

The following graphic is an example of the information that appears on the **Metadata** tab:

General Information License Analysis L	icense Metadata	License Obligations	License Comments		
Hide Empty Metadata Fields				📝 Edit License I	Metadat
License Compatibility Analysis					
List of Incompatible Licenses	GNU General Public L GNU General Public L				
General Compatibility Analysis	such as patent term license. FSF does, h	ense incompatible with ination and indemnificat	on clauses not present in t le 2.0 compatible with GNU	ause of certain "requirements," he older version of the Apache GPL version 3.	
Attribution Compatibility Analysis	None				
Distribution Compatibility Analysis	None				
Modifications Compatibility Analysis	If you consider to m released under GPLv http://thewiki4open GNU General Publ	odify a code released u /2, you should know tha tech.org/index.php/Lice lic License v3.0	t those licenses are NOT C nses_compatibility	it on you project that will be OMPATIBLE. it on you project that will be	
			t those licenses are NOT C		-

6. When you finish viewing and editing the information, click **Save**.

## Viewing, Adding, or Editing a New Obligation



5. Click the Add New Obligation button to define a new license obligation, or click on the Pencil and Paper icon in the Actions column:

Sea	rch:		2				
	Obligation *	Obligation 🔺 🔤		Responsible Organization	Priority	Required	
Ξ	Retain Copyright Notice		Distribution	Other	Medium	No	-
	Follow-up Action Required	the source ve redistribution.	ersion of the redistribution, a	e for Disclaimer.] Typically satisfied by n and if necessary, reproducing such Co in the LICENSE.TXT or third party NOTIC	pyright notice upo	n further	
	License Text Location						
	License Text Fragment	documentatio to use, copy, to whom the s The License of Software in the THE SOFTWA	hereby granted, free of chi- n files (the "Software"), to modify, merge, publish, dist Software is furnished to do copyright notice and permis ne following manner: 	arge, to any person obtaining a copy of deal in the Software without restriction hibute, sublicense, and/or sell copies of so. sion notice shall be included in all copie VITHOUT WARRANTY OF ANY KIND, E IERCHANTABILITY, FITNESS FOR A PA	, including withou f the Software, ar s or substantial p XPRESS OR IMPLI	t limitation the rights ad to permit persons ortions of the ED, INCLUDING BUT	-
ы	↓ Page 1 of 1 ▶		ow All			1-1	lof

- 6. To add a new obligation to a license, go back to the License Edit page.
- 7. Enter the name in the **Search** field of a license for which you want to add a new obligation.
- 8. Click the magnifying glass icon.
- 9. Select a license from the search results, and click the plus icon to expand the license information.
- **10.** Click the **Edit** button at the bottom of the page.
- **11.** Click the **License Obligations** tab.
- 12. Click the Add New Obligation icon. The License Obligation page appears:

Sea	rch:	1	P				
	Obligation 🔺	Triggering Acti	on Responsible Or	ganization Priority	Required		
	Retain Copyright Notice	Distribution	Other	Medium	No		
	Follow-up Action Required	[Supplied by Palamida: See the help page for Disclaimer.] Typically satisfied by not removing copyright notice(s) from the source version of the redistribution, and if necessary, reproducing such Copyright notice upon further redistribution. Copyright notices are generally included in the LICENSE.TXT or third party NOTICES file, as well as in the headers of the source code files.					
	License Text Location						
	License Text Fragment	documentation files (the "Softw to use, copy, modify, merge, pu to whom the Software is furnis	nd permission notice shall be inclu	nout restriction, including withon r sell copies of the Software, a	ut limitation the rights and to permit persons		
N	✓ Page 1 of 1 ▶	Show All			1 - 1	of	

The pull-down menus on the **New Obligation** window can be populated using SQL scripts provided with the product. These menus allow you to specify the following:

• **Obligation**: This is a list of the common types of license obligations provided via a pull-down menu.

- Follow Up Action: This text field allows you to enter specific information related to how users are to address the specific obligation for the current license.
- License Text Location: This allows you specify a path.
- License Text Fragments: You can cut and paste license version and text into these fields and hyperlink information.
- Triggering Action: This is a list of common actions that may trigger a license obligation.
- **Responsible Organization:** This is a list of organizations that typically are responsible for ensuring that required license obligations comply.
- **Priority**: Low, Medium, or High.
- **Required**: Yes or No.

### **Creating a New License**

You create the new license from the License tab. But you add the new license from the Component tab. You can only add licenses to existing components. For details about associating a license with a component, see "Adding New Licenses to Components.

Task	To create a new license, do as follows:
	1. Click <b>Research</b> on the <b>Main</b> menu bar. The <b>Research</b> page appears.

- 2. Select the License tab.
- 3. Click Add New License. The New License dialog appears:

General Info	ormation			
Name				
URL				
Description				
Text				
Category				
Category Is Family?	No	•	Select Family	
		es not have a po		

Note • The Policy field is read-only and contains information regarding any associated policies for this license.

4. Click Save to save the new license.

### **Adding New Licenses to Components**

Before you can add or associate a license with a component, you have to create that license. See Creating a New License for more information.

То	add a license to a component, do as follows:							
1.	Click the <b>Research</b> button on the <b>Main</b> menu bar. The Resea	rch page appears.						
2.	Select the <b>Components</b> tab.							
3.	In the <b>Search</b> field, enter the name of the component with w <b>glass</b> icon.	hich the license is associated and	click the <b>magnifyi</b> r					
4.	4. Locate the component to which you wish to add a license, and click the left-hand <b>Plus</b> icon to expand the componen description.							
5.	Click the Manage Licenses button. The license associated w	ith the component appears.						
6.	<ol> <li>In the License Details for that particular component, click the Add New Component icon to add a new license.</li> <li>Search License dialog appears:</li> </ol>							
	Search License dialog appears:							
	Search License		×					
	Search License	Search:	Add New License Policy Custom					
	Search License       Basic Search     Advanced Search     Filter:     License Name Begins With       Name *       IM     Page     1 of 1     IM	A AND	• Add New License					

### **Deleting a License from Components**

Task	To delete a license from a component, do the following:
	1. Click the <b>Research</b> button on the <b>Main</b> menu bar to open the <b>Research</b> page.
	2. Select the <b>Components</b> tab.

- 3. In the **Search** field, enter the name of the component with which the license is associated.
- 4. Click the magnifying glass icon.

- 5. When you locate the component associated with the license, expand the description by clicking on the left-hand plus icon.
- 6. Scroll down and click Manage Licenses.
- 7. Click the **Delete** icon to delete the license.

# **Using My Settings and Help Functions**

This section provides the steps to access My Settings and Help Functions, which are available to all users:

- My Settings
- Accessing Help

## **My Settings**

# Task

To update your settings, do the following:

1. Log into FlexNet Code Insight and click My Settings in the top right-hand corner. The My Settings page appears.

First Name	Admin	Your Roles			
Middle Name		Scripting Administrator, Sy	vstem Administrat	or	
Last Name	User	Detector Heap Size	1024 MB	v	
Email	admin@admin.com		512 MB		
Job Title			1024 MB	and a second	
			1536 MB		
Business Unit			2048 MB		
Location					
Telephone					
Facsimile					
Login Question	company				
Login Answer	palamida				
Password					
Confirm Password					

2. Enter or update the information in any of the fields.

- 3. Select the appropriate value from the **Detector Heap Size** pull-down menu.
- 4. When you finish entering and updating information, click **Save**.

## **Accessing Help**

**Task** 

#### To access help, do the following:

- 1. Log into FlexNet Code Insight and click **Help** in the top right-hand corner. The **Help** page appears:
- **2.** Select tabs to view links to current application documentation, release notes, known issues, frequently asked questions (FAQ), licensing, legal disclaimers, and about information.

# Conducting Audits & Reviewing Inventory

This section contains the following topics:

- Conducting Audits
- Reviewing Inventory
- Viewing Inventory Items
- Key Inventory Page Items

# **Conducting Audits**

FlexNet Code Insight provides a process that allows the owner to select a project auditor, and the progress of the audit can be managed as part of the project workflow.

After a project is completely defined by an owner and the policies are reviewed with respect to the new project by the policy administrator, the selected project auditor is assigned a task to conduct an audit for the project codebase.

The auditor is responsible for running scans for the workspaces associated with the project, as well as analyzing results and building project inventory based on forensic evidence and automatic OSS component version detection.

Once the project audit is completed by the auditor, the task is closed allowing the project to obtain a compliant status (assuming all detected inventory is compliant as well).

The activities associated with performing a code audit and analysis, as well as publishing project inventory items are detailed in Auditing and Analysis Overview.

# **Reviewing Inventory**

FlexNet Code Insight provides a process by which the project owner can review inventory items and determine whether to make an immediate decision or to require a full review including the completion of a request form. We refer to this process as a Quick Review.

Once the auditor publishes groups from the Detector client, the published groups are available as inventory items in the web client. The project owner can at any time review an inventory item and immediately mark it as approved or rejected for use. Using this operation allows you to skip the full review (workflow) as defined for that project.

Generally, you might use this process as part of a meeting involving all concerned parties: development, legal, security, and any other stakeholders. For example, stakeholders might discuss a set of inventory items ready for review, and then decide if an inventory item should be approved for use, rejected for use, or require a full review including completing the request form associated with the project. If there are any security vulnerabilities associated with the inventory item, a security analyst is required to review these vulnerabilities.

## **Viewing Inventory Items**

#### To view inventory item details, do the following:

- 1. Log into FlexNet Code Insight.
- 2. Click the My Projects button in the Main menu bar.
- **3.** Select the view Magnifying Glass icon in the Actions column next to the project name containing the component for which you wish to view version details. This opens the Project Details tabbed page
- 4. Click on the Inventory tab on the Project Details page.
- 5. Select the inventory item you wish to view, and click on the Magnifying glass icon associated with that item. The Inventory Details tab appears.

Ê

Task

v۷	Inventory	Page	Items
=y	inventory	гаge	items

🕯 Home   🧭 My Projects   🚦	Policies   🕑 Scheduler   😮 Research   🚈 Reports  Welcome Owner   🍰 My Settings   🤣 Help   🖏 Logo			
9 ePortal 1.3 → Inventory	→ prototype 1.6.0.2 (5 of 9 to be Reviewed)			
Component: prototype 1 License: MIT license (also	6.0.2 @ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			
🔑 Inventory Details 🛛 🥥	Comments 🛛 🖓 Questions (0) 🛛 🏖 Checklist Items (0) 📄 🗞 Attachments (0)			
Inventory Name	prototype 1.6.0.2			
Inventory Id	5			
Component Description	Prototype is a JavaScript Framework that aims to ease development of dynamic web applications. Featuring a unique, easy-to-use toolkit for class-driven development and the nicest Ajax library around, Prototype is quickly becoming the codebase of choice for web application developers everywhere			
Disclosed	No			
Review Status	Approved This use of this inventory item has been approved via a complete IP review. Click here to view the associated request details.			
Number of Files	1 File 0			
Auditor Notes & Detection Evidence	Internal: Detection Confidence: 100% Supporting Evidence: Multi-Indicator: System rule 100041: MID rule for prototype External: None			
Possible Licenses	MIT license (also X11) & 👩 🏴			
As-Found License Text	View As-Found License Text			
Inventory Metadata	View Inventory Metadata			
Inventory Policy	I <sup>II</sup> No Policy This inventory item does not have a matching policy.			
Review History	prototype has previously been approved 2 times and rejected 0 times.			
Detected By	System			
Last Updated	01/05/2012 10:08			
	Return to Inventory List			

The Inventory Details tab contains all the information necessary to determine whether to approve, reject, or schedule a full review for the item.

## **Key Inventory Page Items**

Key items on the Inventory page are presented in the following tables.

### **Component Details**

Component details and their associated icons are as follows:

Component		Description		
Available Versions icon	0	List of available versions as well as the count of associated security vulnerabilities.		
Component Metadata icon	0	Show the component metadata dialog;		
Component Policy Flag icons	۳	Component always approved for use.		
	۳	Component always rejected for uses.		

Component	lcon	Description
	۲	Component has unknown policy since it depends on use.
	h	Component does not have a matching policy.
Approval Status icons	0	Component has been previously Approved.
	0	Component has been previously Rejected.
Encryption Details	9	Details related to whether or not encryption is required.
Security Vulnerability Details icon		Vulnerabilities associated with a specific version.

### **License Details**

License details are available for viewing by clicking on associated License icons.

Component	lcon	Description
License Details icon	Ð	Includes the license text, as-found license text, license comparison, license analysis (if available), license metadata (including compatibility analysis), license obligations, and license comments.
Component Policy Flag icons	۳	License always allowed.
	۳	License never allowed.
	۳	License has unknown policy since it depends on usage.
	lhu	License does not have matching policy.

## **License Text Comparison**

The **License text** comparison feature allows you to compare the following types of license text associated with a given inventory item:

- License family
- Expected license
- As-found license

#### To compare license types, do the following:

¢

Task

- 1. To view an inline comparison of two license texts associated with an inventory item, go to an inventory item.
- 2. Click the View License Details icon () next to the license name. The License Comparison page appears:

Scriptaculous License								l
As-Found License Text	Expected License Text	License Family	Comparison	License Metadata	License Analysis	License Obligations	License Compatibility	
	Compare	As-Found License	Text	to License Family T	rext 💌	Compare		
		As-Found l	<b>icense</b> comp	ared to <b>MIT Lic</b>	ense Family			
Copyright <mark>(c) <yea< mark=""></yea<></mark>	<del>rə ceopyright hold</del> ı	<del>ers&gt;<u>@</u>2005-2</del> 1	008 Thomas Fi	uchs (http://sc	ript.aculo.us, h	ttp://mir.aculo.u	<u>ड</u> ो	3
(the "Software"), t oublish, distribute, subject to the follo The above copyrigi THE SOFTWARE IS THE WARRANTIES AUTHORS OR COPY	ht notice and this p PROVIDED "AS IS", OF MERCHANTABILI RIGHT HOLDERS BE OR OTHERWISE, AR	rare without re sell copies of permission notion WITHOUT WA ITY, FITNESS F LIABLE FOR A	striction, inclu the Software, ce shall be inc RRANTY OF AL FOR A PARTICU NY CLAIM, DA	ding without lin and to permit p luded in all copi NY KIND, EXPRE JLAR PURPOSE , MAGES OR OTH	nitation the righ persons to whor ies or substanti SS OR IMPLIED AND NONINFRIN IER LIABILITY, V	ts to use, copy, n the Software is al portions of the , INCLUDING BUT GEMENT. IN NO VHETHER IN AN A	modify, merge, s furnished to do so e Software. NOT LIMITED TO EVENT SHALL THE ACTION OF	3,

- 3. To compare two different license text types, select the two license text types to compare from the pull-down menus:
  - License Text: The license text for the selected license from the FlexNet Code Insight Compliance Library.
  - As-Found License Text: The value of the As-Found License Text group field in Detector that was entered by the auditor.
  - License Family: The license text of the license family to which the selected license belongs.
- 4. Click the Compare button.

**Note** • If a license text type is empty, it isn't viewable.

## **Other Inventory Page Header Items**

Items that appear near the top of the Inventory page are as follows:

#### Table 6-1 • Page Header Items

Item	Description
License	Allows for inventory reviewer to override the selected license for the inventory item. The possible values for the license pull-down menu come from the possible license list as defined by the auditor via the FlexNet Code Insight client.
Priority pull-down menu	Project owner may change this value, and others will see it as a read-only fields
Remediation status	Denotes the current state of scheduled remediation work for this inventory item
Review Status/Change Inventory Status Section	Shows the current review status of the inventory item
	Project owner has the option of marking the inventory item as approved for use, rejected for use, or schedule a full review.
	If a full review is scheduled, an option to associate an existing request or create a new request will be available.
	A security analyst may see an option to review security vulnerabilities if any are associated with the component version, and the inventory item requires a full review. Otherwise, a view vulnerabilities button will be available.

### **Inventory Item Tabbed View**

The following tabbed views are associated with Inventory:

#### Table 6-2 • Tabbed View Items

Item	Description	
Comments	List of comments for the current inventory item	
Questions	List of questions and answers for the inventory item	
Checklist Items	List of check list items of type general, legal, remediation, or security	
Attachments	List of attached files for the current inventory item	

## Additional Inventory Details on Tabbed Views

Additional information available for viewing is as follows:

#### Table 6-3 • Addition Details

Item	Description
Inventory Name	Name of the inventory item (as entered by the system or auditor)
Inventory ID	ID of the inventory item (unique to the system)
Component Description	Description of the associated component
Disclosed	This is a yes or no value that indicates whether or not the inventory item was disclosed before the audit or whether the finding was a surprise.
Review Status	Detailed explanation of the current review status of the inventory item as well as hyperlinks to the policy or request that was used to automatically review the inventory item (if applicable)
Number of Files	List of files associated with the inventory item (ordered by file path or workspace name)
Auditor Notes & Detection Evidence	Auditor notes along with explanation of how the inventory item was detected (if detected by is System)
Possible Licenses	List of all licenses associated with component or version. This list can be modified by the auditor via the Detector client, or by any QuickReview™ Facilitator via the web UI.
As-Found License Text	The license text as found in the codebase by the auditor.
Inventory Metadata	Link to the inventory metadata dialog.
Inventory Policy	Matching policy with a details link including the component name, version, and license
Review History	Number of times, historically, requests for the inventory item were approved and rejected in the past.
Detected By	Name of auditor who created the inventory item ("System" means that this item was automatically detected by the system.)
Last Updated	Date that the inventory item was last updated

## **Viewing Source Code Fingerprint Match Highlights**

FlexNet Code Insight provides the ability to view ASCII text file contents associated with a given inventory item as well as source code fingerprint match highlights (if available).

Task	

To view the contents of a file along with source code fingerprint match highlights, do the following:

1. Click the View Inventory Files icon (<sup>1</sup>) in the Number of Files field. The View Inventory Files page appears:

🚱 Home   🎲 Administration	🔹   🃁 My Projects   🏮 Policies   🕑 Scheduler   😝 Research   🔀 Reports 🛛 🛛 Welcome Alex   襊 My Setti	ngs   🛟 Help   🐗 Logout		
$\bigcirc$ ePortal 1.3 $\rightarrow$ Inventory	→ opendx (13 of 20 to be Reviewed)			
Component: opendx & ເ		eady for Review		
🔑 Inventory Details 🏼 🥥	Comments (0) 🛛 🤣 Questions (0) 🛛 🌋 Checklist Items (0 of 1 Not Completed) 🛛 📎 Attachments (0)			
Inventory Name	opendx			
Inventory Id	17			
Component Description	Pert Description Open Visualization Data Explorer is a visualization framework that gives users the ability to apply advanced visualization and analysis techniques to their data. These techniques can be applied to help users gain new insights into data from applications in a wide variety of fields including science, engineering, medicine and business. Data Explorer provides a full set of tools for manipulating, transforming, processing, realizing, rendering and animating data and allow for visualization and analysis methods based on points, lines, areas, volumes, images or geometric primitives in any combination. Data Explorer is discipline-independent and easily adapts to new applications and data. The integrated object-oriented graphical user interface is intuitive to learm and easy to use.			
Possible Licenses	IBM Public License v1.0 🕫 🝺 🏴	Edit Possible Licenses List		
As-Found License Text	View As-Found License Text			
Number of Files	1 File 🧿			
Review Status	A Ready for Review This inventory item is ready to be reviewed.			

Auditor Notes None

2. Click the View icon next to the desired file.

pendx	Contains 1 Evidence File			>
			Group by : None	~
View	Path 🔺	Server	Workspace Name	
Θ	C:\Cleanroom\ePortal-1.3\src\autoglyph.c	server1	ePortal_13_src	
14-4	Page 1 of 1 🕨 🕅 🖓 Show All			
		Close		

If the auditor marked several matched files as best source matches, you will see a pull-down menu from which you can select the desired remote matched file for comparison. If the auditor did not mark any matches, the system will show the top match automatically. A new **View Evidence File** window opens with the selected scanned file on the left and the selected (or best) remote matched file on the right.

CodeRank :	87.35%	Coverage: 100%	Clustering :	53.77%		Uniqueness: 100%	Mat	ches: 159	
					Er	nable syntax highlighting:	File Viewer:	Split Vertically	
	:\Cleanroom\ePortal	-1.3\src\autoglyph.c		Remo	te File : open	ndx:autoglyph.c			
No         No           41         whli           42         if (i:           43         if (:           44         else           45         else           46         else           51         if (:           52         or           53         }           55         >           56         or           661         662           662         666           67         666           666         or           77         #if II           78         %           80         // jr:           81         // jr:           82         i++;           86         i++;           87         Vzpr           88         i           87         vzpr	<pre>le i &lt; 29 c6 tv; saluhaitvoe string idumeritvoe string[count voe string[count voe string[count if (return:</pre>	<pre>pe string[i] '= '\0') { nd[i]); nd[i]); pe tolower(type_string[i]; pe type_string[i]; pe type_string[i]</pre>	<pre>pt-To: %s\r\n", = poid : loginname g command line, :Priority: Low\:Priority: High ]) ( g, 1, 12); ps: ");</pre>	$\begin{array}{c} 135\\ 136\\ 137\\ 139\\ 140\\ 142\\ 144\\ 143\\ 144\\ 145\\ 146\\ 145\\ 151\\ 152\\ 153\\ 154\\ 155\\ 156\\ 157\\ 158\\ 159\\ 160\\ 161\\ 162\\ 166\\ 166\\ 166\\ 166\\ 166\\ 166$	<pre>} if ((qua stropy /* tur i = 0; count i = 0; count if (isi type else type count } if (vy type_s) } if (vy type_s) } else { stropy(t } /* scale * if(scal DXSetE goto e } else { scale se AutoSIze } /* the ind if (class</pre>	<pre>lity==-1) &amp; &amp; (!type_ (type_string,type); in type string to lo = 0; (i &lt; 29 &amp; &amp; type_string[i]) upper(type_string[i] _string[count]= tol _string[count]= tol _string[count]= typ +; pe_string[count]= typ it+; string[count]= '.' ;string[count]= '.' ;string[count]=</pre>	<pre>*/ wer case */ ing[i] != '\0') { } j); ower(type_string[ } ) ( e_string[i];  d"); d"); d"); METER, "#10090", METER, "#10090", */ P) (</pre>	"scale");	

- 3. Review the top header for the corresponding source match heuristics for the scanned file. These include FlexNet Code Insight CodeRank<sup>™</sup>, Coverage, Clustering, Uniqueness, and Matches, the number of source matches.
- **4.** Below the top header, you can choose to check the Enable syntax highlighting checkbox. This allows for highlighting in programming-language-specific color coding (as you might see in a text editor).
- 5. Review the File Viewer option. The pull-down allows you to split the dual-pane view horizontally or vertically.
- 6. Click the **minus** icon in the top-right of the **Remote File** panel to close the panel and show only the contents of the scanned file.

#### Chapter 6 Conducting Audits & Reviewing Inventory

Key Inventory Page Items

81

Reviews & Approving

# Performing Quick Reviews & Approving or Rejecting Inventory

This section explains how to perform a quick review of inventory and mark it as approved or rejected:

- Performing Quick Reviews & Marking Inventory
- Scheduling Inventory for Full Review

# **Performing Quick Reviews & Marking Inventory**

#### Task

Ê

To perform a quick review and mark inventory as approved or rejected, do the following:

- 1. Log into FlexNet Code Insight as an owner.
- 2. Click the My Projects button in the Main menu bar.
- Select a project for which you want to review inventory by clicking on the associated view Magnifying Glass icon in the Actions column. A Project tabbed view appears that includes the Summary, Workspaces, Inventory, Requests, Tasks, Policies, and Comments tabs.

🕯 Home   🥲 My Projects   🚦	olicies   🛞 Scheduler   🔮 Research   🕅 Reports	Welcome C	Owner	🛃 My Settings 🛛	🕽 Help	Log
ePortal 1.3						
Summary Workspaces	wentory Requests Tasks Policies Comments					
ld	1					
Vame	ePortal 1.3					
feam	Engineering					
Owner	Owner Smith					
Auditors	Alex Rybak, Auditor Smith					
Security Analysts	Alex Rybak					
Observers	Observer Smith, Super User					
QuickReview Facilitators	Alex Rybak, Owner Smith, Super User					
Advanced Options	Apply Policies to Inventory: Yes Request Form: F	y Emails: Never Reminder Emails: Never Palamida Default Short Request F to Select First Reviewer: No	orm De	finition		
Project Metadata	View Project Metadata					
Aliased Projects	There is no aliased project for this project.					
Child Projects	There are no child projects for this project.					
Status	In Progress					
Progress	Audit  Subscription  Subscript	wed wiewed w, 3 approved, and 2 not yet reviewed 1, and 7 none required)		ect Inventory Snapsh	ot) Sca	an Project

- 4. Click the Inventory tab.
- 5. Choose the inventory item you wish to review and click the Magnifying Glass icon associated with the component you wish to review. The **Project Component Inventory Details** page appears:

ePortal 1.3 → Inventory	→ mcrypt 2.6.8 (1 of 9 to be Reviewed)	
Component: mcrypt 2.6.8	B @ @ @ Priority: 2 - High 💌	
	Comments 2 Questions (0) 2 Checklist Items (0) 🗞 Attachments (0)	Approve Inventory Item
Inventory Name	mcrypt 2.6.8	Schedule Full Review
Inventory Id	2025	
Component Description	mcrypt, and the accompanying libmcrypt, are intended to be replacements for t support an ever-wider range of algorithms and modes.	the old Unix crypt, except that they are under the GPL an
Disclosed	No	
Review Status	A Ready for Review	
	This inventory item is ready to be reviewed.	
Number of Files		
	This inventory item is ready to be reviewed.	
Possible Licenses	This inventory item is ready to be reviewed. 1 File 💿	
Number of Files Possible Licenses As-Found License Text Inventory Metadata	This inventory item is ready to be reviewed. 1 File (a) GNU General Public License v3.0 (27) (a)	
Possible Licenses As-Found License Text Inventory Metadata	This inventory item is ready to be reviewed. 1 File (a) GNU General Public License v3.0 (P) (a) View As-Found License Text	
Possible Licenses As-Found License Text Inventory Metadata Inventory Policy	This inventory item is ready to be reviewed.  1 File  GNU General Public License v3.0 P GNU General Public License Text View As-Found License Text View Inventory Metadata  M No Policy	
Possible Licenses As-Found License Text	This inventory item is ready to be reviewed.  1 File  GNU General Public License v3.0 P GNU General Public License Text View As-Found License Text View Inventory Metadata  P No Policy This inventory item does not have a matching policy.	

- 6. Select the Approve or Reject options in the Change Inventory Status... menu in the top-right corner of the page.

Note • A system-generated comment is added to an inventory item to record when a review status change occurs.

# **Scheduling Inventory for Full Review**

# Task

#### To schedule inventory for a full review, do as follows:

- 1. Log in to FlexNet Code Insight as an owner.
- 2. Click the My Projects button in the Main menu bar.
- Select a project for which you want to review inventory by clicking on the associated view Magnifying Glass icon in the Actions column. A Project tabbed view opens which includes the Summary, Workspaces, Inventory, Requests, Tasks, and Policies tabs.
- 4. Select the Inventory tab.
- 5. Select the inventory item you wish to review and click on the Magnifying Glass icon associated with this component. The **Project Component Inventory Details** page appears.
- 6. Select the Schedule Full Review option in the Change Inventory Status... pull-down menu located at the top-righthand corner of the page.

_		Ъ
-	-	-
-	-	-

**Note** • Scheduling an inventory item for full review kicks off the full workflow. It creates an IP review task for the project owner as well as a security review task for the security analyst if the inventory item has any associated security vulnerabilities.

Chapter 7 Performing Quick Reviews & Approving or Rejecting Inventory

Scheduling Inventory for Full Review



# **Reconciling Inventory**

The following topics appear in this section:

- What is Reconciling Inventory?
- Associating Inventory with Component Requests
- Associating Inventory with Requests across Projects
- Unassociating a Request from an Inventory Item
- Creating a New Component Request

# What is Reconciling Inventory?

Once the project owner schedules an inventory item for a full review, the item must be associated with a component request to determine its compliance state. The following are the scenarios that may occur as part of this process:

- An approved component request is available to permit the use of the inventory item if the intended use of the item meets the predetermined conditions for use. In this case, the association to this request makes the inventory item IP-Compliant, and the project workflow advances to the next phase.
- A rejected component request is available that matched the conditions under which the inventory item will be used. In this case, an association to this request makes the inventory item IP Non-Compliant. This scenario requires either the requester to change the intended usage of the component, and then submit the request for another review of the amended component request, or a remediation. A remediation may require that the component be modified to a different version or an alternate component altogether.
- There is no existing component request for the inventory item, and a new component request is created to allow for a review of the intended usage of the component. The result of the component request cycle is an approved or rejected component request.

# **Associating Inventory with Component Requests**

# Task

To associate a compliant inventory item to a request, do as follows:

- 1. Log in to FlexNet Code Insight.
- 2. Click the My Projects button.
- 3. Select the project for which you would like to review requests and click on the magnifying glass icon (<sup>[]]</sup>) in the **Actions** column.
- 4. Select the Inventory tab.
- 5. Select an inventory item with a status *Pending Review* for which you would like to associate an existing request (option available to Owner or Participant) or create a new request (option available to Requesters only).
- 6. Click on the magnifying glass icon (<sup>[]]</sup>) associated with this inventory item in the **Action** column.
- 7. Select the **Create/Associate Request** option from the drop down menu.



The result will be one matching request, no matching requests or multiple matching requests:

- If there is one matching request in the system, you can click **Associate** to associate the request with the inventory item. If the request is an *Approved* state, the item is automatically approved based on the association.
- If there are no matching requests, a message will be displayed indicating that there are no matches. If you have the role of Requester for the current project, you can click **Create a New Request** to create a request that matches the inventory item.
- If more than one existing request matches the inventory item, a list of possible requests appears:

ld	Project	Requester	Component 🔺	License	Status	Actions
6	Project1	Owner One	itext (5.1.2)	Other/Commercial	Pending	Q
5	Project1	Owner One	itext (5.1.2)	Other/Commercial	Pending	Q
14	Page	1 of 1   ▶ ▶    22	Show All			1-2

**8.** Select the request that matches the inventory item and press the **Associate** button to make the request-inventory item association.

If an inventory item has an associated request, the **Inventory Details** tab will have the **View Associated Requests** option in the upper right-hand corner.

Component: itext 5.1.2 @	Priority: 6 - Not Set	📤 Pending Review				
License: Other/Commercia	▼ 💿 🏴 Remediation: Not Required	(Change Inventory Status				
		A Reset to Ready for Review				
🔑 Inventory Details Thir	d-Party Notice 🛛 🥥 Comments (7) 🖓 Questions (0) 🖓 Checklist Items (0) 📎 Attachments (0)	View Associated Request				
Inventory Name	iText 5.1.2					
Inventory Id	22					
Component Description	Download iText®, a JAVA PDF library. iText is a PDF library that allows you to CREATE, ADAF the Portable Document Format (PDF):- Generate documents and	T, INSPECT and MAINTAIN documents in				
Possible Licenses	GNU Affero General Public License v3.0 ଜୁ 👩 🏴 Other/Commercial ଜୁ 👩 🟴	Edit Possible Licenses List				
As-Found License Text	View As-Found License Text					
Number of Files	0 inventory files (including files inside archives)					
Review Status	Pending Review This inventory item is pending a complete IP review. The request associated with this inventory in Owner One Click here to view the associated request details.	tem is currently pending review by:				

## Associating Inventory with Requests across Projects

In some cases, there may be a need to associate an inventory item to a request located in a different project such as the Global Request Project. This type of association can be made if you have Product Catalog configured and the inventory item and request are both associated with the same Product Catalog item.

Task

Ê

To make the associate a request to an item in another Product Catalog product, do the following:

- 1. Associate the Product Catalog Item with the given project.
- 2. Associate the Product Catalog item with the request.
- 3. From the associated project, create an inventory item that matches the request component, version and license.
- 4. Schedule a Full Review for the inventory item and select the option to Associate the Request.
- 5. The request is available in the search results based on the Product Catalogassociation.

## **Unassociating a Request from an Inventory Item**

Task	k To unassociate a request from an inventory item, follow these steps:					
	1.	Open the inventory item and select View Associated Request from the <b>Change Inventory Status</b> menu in the upper right-hand corner. The <b>Request Details</b> page appears.				

2. Press the Unassociate button on the bottom of the Request Details page to remove the association.

## **Creating a New Component Request**

To create a new component request, see Creating a Component Request.

Chapter 8 Reconciling Inventory Creating a New Component Request

# Requesting Permission to Use a Component

This section contains the following topics:

- Requests
- Changing the Request Form
- Creating a Component Request
- Viewing Requests
- Viewing Request Details
- Cloning a Request

### **Requests**

When a project is set up in the system, the number of review levels and team members responsible for reviewing component requests are established by the project owner. The policy administrator is responsible for setting up automatic policies for component/license combinations, which automatically assign the new request a status of approved, rejected, or determines that the request requires manual review.

If a requester submits a new request for a component/license, and no policy is associated with that new request, a workflow is created based on the project attributes. The system automatically sends email notifications to the users responsible for reviewing the request.

Upon submission, the request is assigned to the first-level reviewer for action. If the request is approved, it is sent to the next person in the workflow responsible for reviewing it. Once all reviewers approve the request, it moves to history. If the component has conditions for use, once the request is approved by all reviewers, the request is automatically sent back to the requester for review and acknowledgment of the conditions for use. If a request is rejected, the workflow stops immediately, and the request is completed and moved to history. For each step in the workflow, the system sends email notifications to the appropriate requesters and reviewers notifying them of the action needed or action taken.

The possible request statuses are as follows:

Draft: This is a work-in-progress component request saved as a draft and not submitted for review.

- Pending: This is a component request submitted for review, and a workflow is consequently created.
- **Approved**: This status means that the component request is approved by all reviewers and all required conditions for use are reviewed and acknowledged by the requester.
- Rejected: This means that at least one reviewer rejected the component request.
- FlexNet Code Insight provides the ability to customize the appearance of the **Request Dashboard**. For more information, see Customizing the Request Dashboard.

## **Changing the Request Form**

FlexNet Code Insight supports multiple request form definitions. A project can only be associated with a single request form. The product is shipped with two SQL scripts containing a sample definition of a short and long component request form.

**Note** • There are several built-in attributes that are required for each request form definition. They are discussed in the following section. Furthermore, the last Additional Information tab is fixed and cannot be changed. An administrator may change the Component Request form input fields (attributes) and/or add additional tabs.

Via a database SQL script, the following changes can be made to the request form:

- Add or remove tabs.
- Add or remove attributes.
- Modify the fields of the attributes, including the text, help text, activity status (required, optional, or conditional), sequence and input type (for example, changing from text box to a list box with pre-defined values).

The Component Request form input fields provide you with the following:

- Information a reviewer needs to make an informed decision as to whether you can allow a requester to use third-party components in the development process
- Those users with requester role permissions can create a new component request and save it as a draft request: This way, requesters have the option of editing and completing the request at a later date.

### **Required Request Form Input Fields (Attributes)**

There are several mandatory input fields for each request form definition. These fields are required in order to have a valid request form definition. The fields can be located on any tab in the request form. Each of these fields require an input type = W (INPUT\_TYPE\_ column in the PAS\_REQ\_DEF\_ATTR table) which stands for built-in widget. The field names (NAME\_ column in the PAS\_REQ\_DEF\_ATTR table) must be equal to those shown in the table below.

Table 9-1 • Input Fields

Field Name	Description
_palamida_projectName	Pull-down menu to select the project name, the value will be pre-selected if request is initiated from within a project

#### Table 9-1 • Input Fields

Field Name	Description
_palamida_componentName	Search widget to select the appropriate component for which the request is being made
_palamida_componentVersion	A constrained pull-down menu with version names associated with the selected component
_palamida_licenseName	A constrained pull-down menu with license names associated with the selected component
_palamida_reviewDeadline	A calendar widget to select the review deadline for the request: The current date is selected as the default value

# **Creating a Component Request**



#### To create a component request, do as follows:

1. Log in to FlexNet Code Insight as a *Requester*:



2. Click My Projects, and then click the magnifying glass in the Actions column:

	🕑 Scheduler   \rm 🛛 Research   🌌 Repo	113	WGA	come <mark>Requeste</mark>	II ay my 5	enniga   🍕	Alleib   Albir
📁 My Projects							
Basic Search Advanced Search   Filter	In Progress Projects 🗸 Search	1		2			
Name 🔺	Team	Owner	Status	Inventory	Requests	Tasks	Actions
ePortal 1.3	Engineering	Owner Smith	In Progress	9	8	0	D
	Engineering	Alex Rybak	In Progress	9	8	0	B

3. Select the Requests tab. The Request Dashboard appears.

🗹 Requests R	tepository									
Basic Search	Advanced Search	h								O Add New Reques
Request Filter:	All Requests	Y Project Filter.	~ k	leyword Search:		Q				
Id	Project	Component	License	R	equester	Current Assignee +	Status	Pending Review	Reviewed By	Created On
4	p2	zlib (1.2.3)	zlibflibpng License	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
8	p2	junit (4.10)	JUnit License	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
12	p2	junit (3.8.1)	Common Public License	R	equester3 Three	None	Approved		Manual	07/26/2017 11:02
16	p2	junit (3.8.1)	Common Public License	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
20	p2	springframework (2.5.1)	Apache License 2.0	R	equester2 Two	None	Approved		Manual	07/26/2017 11:02
24	p2	jquery (2.0.1)	MIT License (also X11)	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
40	p2	jquery (2.0.2)	MIT License (also X11)	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
44	p2	jquery (2.0.1)	MIT License (also X11)	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
52	p2	sweetinsanity (unknown)	MIT License	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
11	p2	junit (3.8.1)	Common Public License	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
15	p2	junit (3.8.1)	Common Public License	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
19	p2	springframework (2.5.1)	Apache License 2.0	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
23	p2	mysql-connector-j (3.1)	GNU General Public License v2.0	R	equester1 One	None	Approved		Manual	07/26/2017 11:02
39	p2	jquery (2.0.1)	MIT License (also X11)	R	equester1 One	None	Approved		Manual	07/26/2017 11:02

#### 4. Click Add New Request. The New Request page appears:

ePortal 1.3 -	→ Request → New Request								
eneral Usage	e Additional Information								
Comp	ponent Name:								
		Search Component	Any Component	View Component Versions	View Component Metadat	ta)			
Proje	ect Name:								
ePorta	al 1 3				Farmer				
Revie 04/25/	ew deadline: - MM/DD/YY	YY			×				
04/25/	ew deadline: - MM/DD/YY	"cryptography", or	otherwise con	tain any parts or con		able of pe	erforming "infe	ormation	
04/25/	this component perform tity" functions? (More Inf	"cryptography", or prmation)			nponents that are cap	able of pe	erforming "info	ormation	
04/25/ ■ El Does secur ○ Yes ■ Will th ○ Yes	ew deadline: - MM/DD/YY 2012 this component perform ity" functions? ( <u>More Inf</u> s © No this component be modif	"cryptography", or ormation) ied, re-compiled, o			nponents that are cap	able of pe	erforming "info	ormation	
04/25/ ■ El Does secur ○ Yes ■ Will th ○ Yes	ew deadline: - MM/DD/YY <sup>(2012</sup> this component perform ity" functions? ( <u>More Inf</u> s © No this component be modif s © No	"cryptography", or ormation) ied, re-compiled, o			nponents that are cap	able of pe	erforming "info	ormation	

- 5. Enter the appropriate information in the fields.
- 6. Select the Additional Information tab.
- 7. Click Post Comment, and enter any relevant comments in the Additional Comment field:

New Comment		×
Comment		
<ul> <li>Visibility Type</li> </ul>		
	Post Cancel	

8. Attach a file if you want.

9. Submit the new request, or click **Save as Draft** to do additional work on your new request before submitting it for review.

# **Viewing Requests**

# Task

To review requests related to your role, do as follows:

- 1. Log into FlexNet Code Insight.
- 2. Click My Projects, and then click the magnifying glass in the Actions column.
- 3. Select the **Requests** tab.
- 4. If you log in as an **Owner**, you can select **All Request**, **Completed Requests**, **My Submitted Requests**, **Requests**, **Requests**, **Requests**, **My Submitted Requests**, **Requests**, **Request**, **Request**,

ePortal	1.3									
Summary	Workspaces Inve	entory	Requests	Tasks	Policies	Comments				
Basic Sea	rch Advanced Search	Filter:	All Requests		~	Search:	P			
ld 👻	Requester	Comp	All Requests			nse	Review Deadline	Status	Reviewed By	Actions
15	Alex Rybak	VMw				ptaculous 1.8.1 License	01/24/2012	Approved	Manual	0
10	Alex Rybak	itext (		My Submitted Requests		J Affero General Public License v3.0	01/05/2012	Pending	Manual	Ø
8	Alex Rybak	proto	Requests Requiring My Action Associated Requests		uon	license (also X11)	12/29/2011	Approved	Manual	0
7	Alex Rybak zlib (1			nassociated Requests		libpng License	12/26/2011	Pending N	Manual	D
6					MIT	license (also X11)	11/02/2011	Rejected	Manual	đ
5	Alex Rybak	Any Component (Any Version) MIT			MIT	license (also X11)	11/02/2011	Approved	Manual	Ø
4	Alex Rybak scriptaculous (1.8.1) scrip		iptaculous 1.8.1 License	09/26/2011	Approved	Manual	đ			
1	Alex Rybak	iboss	(5.2.5)		GN	U Lesser General Public License v2.1	08/16/2011	Pending	Manual	a

Note • If you are logged in as a Requester, you see another filter at the bottom of the My Draft Requests list.

## **Viewing Request Details**

# Task

To view request details, do the following:

- 1. Log into FlexNet Code Insight as a Requester. The Requester Home page appears.
- 2. Click My Projects. The My Projects page appears.
- 3. Choose a project, and click the associated **magnifying glass** in the **Actions** column.

4. Select the Request tab:

Summary	y Inventory Re	quests Tasks Policies Comme	ents				
Basic S	earch Advanced Sea	rch   Filter: All Requests	Search:	Q		O Add I	New Request
id 👻	Requester	Component	License	Review Deadline	Status	Reviewed By	Actions
10	Alex Rybak	itext (5.1.2)	GNU Affero General Public License v3.0	01/05/2012	Pending	Manual	0
8	Alex Rybak	prototype (1.6.0.2)	MIT license (also X11)	12/29/2011	Approved	Manual	
7	Alex Rybak	zlib (1.2.1)	zlib/libpng License	12/26/2011	Pending	Manual	٥
6	Alex Rybak	Any Component (Any Version)	MIT license (also X11)	11/02/2011	Rejected	Manual	0
5	Alex Rybak	Any Component (Any Version)	MIT license (also X11)	11/02/2011	Approved	Manual	
1	Alex Rybak	jboss (5.2.5)	GNU Lesser General Public License v2.1	08/16/2011	Pending	Manual	0

5. Select the magnifying glass next to the request you want to view. The General Usage tab appears:

neral (	Usage Additional Information					
C	Component Name:					
it	text (id:4744) View Component Versions View Component Metadata					
C	Component Version:					
5	5.1.2					
	License Name:					
G	GNU Affero General Public License v3.0 View License Details					
P	Project Name:					
e	Portal 1.3					
R	Review deadline:					
0	01/05/2012					
	Does this component perform "cryptography", or otherwise contain any parts or components that are capable of performing "information security" functions? ( <u>More Information</u> )					
N	No					
۷	Will this component be modified, re-compiled, or repackaged with any other software?					
N	No					
V	What is the intended usage of this component?					
C	Development Tool (Compiler, IDE, Code Generator)					
	Recall Change Requester Cancel					

## **Cloning a Request**

Cloning a request saves the requester the time of filling in an entirely new request form for what might amount to making a small change for the request of a very similar component. If you would like to clone a request, do as follows.

# Task To clone a request, do the following. 1. Log into FlexNet Code Insight as a Requester.

- 2. Click My Projects.
- 3. Choose a project, and click the associated magnifying glass in the Actions column.

- 4. Select the Requests tab.
- 5. Click the **Magnifying glass** associated with an approved request you wish to clone. The **Requests Details** page appears.

**Note** • The **Clone** button is only active on requests that have completed review.

**6.** At the bottom of the **General Information** tab, click **Clone**. The system clones the request, and you will receive a notification at the top of the **Request** page that states the request, identified by a number, has been cloned.

**Note** • If the request form definition has changed since the original request was created, the cloned request will map as many input fields and their values as possible. A system-generated comment will be added to the cloned request with a list of input fields that the system is unable to map.

#### Chapter 9 Requesting Permission to Use a Component

Cloning a Request



# **Customizing the Request Dashboard**

This section provides information and procedures to customize the **Request Dashboard**:

• Adding the Assigned Date Column

# **Adding the Assigned Date Column**

FlexNet Code Insight provides the ability to add an **Assigned Date** column to the **Request** dashboard. The Assigned date appears when the request was last assigned to the current assignee. The column makes it easier to identify requests that are delayed in the review process and need to be prioritized. To add the **Assigned Date** column, follow these instructions.



#### To add the Assigned Date column, do the following:

 Add the following text to the requests.web.json file (located in <FNCI\_ROOT\_DIRECTORY>/config/core/ requests.web.json). You may change the name of the column heading by modifying the "header" value and change the column order by modifying the "positionIndex" value.

```
'dataIndex": "assignedDate",
    "derived": true,
    "positionIndex": -2,
    "header": "Assigned On",
    "width": 150
}
```

**Note** • The -2 refers to the  $2^{nd}$  position from the right.

2. Launch a new browser session and navigate to the Requests dashboard, which has the Assigned Date column.

**Note** • Although this modification does not require a server restart, you may want to clear your browser cache if the column does not appear

#### Chapter 10 Customizing the Request Dashboard

Adding the Assigned Date Column



# **Reviewing Pending Requests**

This section explains how to review pending requests. It contains the following section:

• Pending Requests

# **Pending Requests**

Reviewing requests is a part of a project request workflow. Any user in the system with the reviewer permissions is eligible for selection as a reviewer in a review level.

- Any reviewer in the review level may review a pending component request, thereby locking out the other peer reviewers.
- Once a request is reviewed, the request advances to the next review level as defined in the project workflow.

## **Reviewing Pending Requests from the My Tasks Tab**

Task	То	To review pending requests from the My Tasks Tab, do the following:								
	1.	Log into FlexNet Code Insight as a <b>Reviewer</b> . Ensure the application administrator has set up your user account with Reviewer permissions.								
	2.	Click the <b>Project</b> button on the <b>Main</b> menu to see a list of your projects.								
	3.	Click the magnifying glass icon associated with the project for which you want to review requests. The <b>Project</b> page appears.								
	4.	Click the <b>Request</b> tab. The <b>Review Task</b> page appears.								

Summary	Inventory Reques	sts Tasks	Policies Comme	ints				
Basic Se	arch Advanced Search	Filter: All Re	quests	Search:	Q			
ld 🔻	Requester	Component		License	Review Deadline	Status	Reviewed By	Actions
6	Alex Rybak	Any Compor	ent (Any Version)	MIT license (also X11)	11/02/2011	Rejected	Manual	
5	Alex Rybak	Any Compor	ent (Any Version)	MIT license (also X11)	11/02/2011	Approved	Manual	
4	Alex Rybak	scriptaculou	s (1.8.1)	scriptaculous 1.8.1 License	09/26/2011	Approved	Manual	
1	Alex Rybak	jboss (5.2.5)		GNU Lesser General Public License v2.1	08/16/2011	Pending	Manual	D

5. To review a request assigned to you, click the associated magnifying glassicon. A **Review** page appears on which you can view the associated request:

neral Usag	ge Additional Information							
	nponent Name: t (id:4744) View Component Versions View Component Metadata							
Con 5.1.2	npone <mark>n</mark> t Version: 2							
1111	ense Name: J Affero General Public License v3.0 View License Details							
	Project Name: ePortal 1.3							
	riew deadline: 15/2012							
	Does this component perform "cryptography", or otherwise contain any parts or components capable of performing "information security" functions? (More Information)							
	Will this component be modified, re-compiled, or repackaged with any other software?							
Wha	What is the intended usage of this component? Development Tool (Compiler, IDE, Code Generator)							
Deve	*							
Deve	⇒							

## **Reviewing Pending Requests from the Requests Tab**

Task	To review pending requests from the Requests tab, do the following:
	1. Log into FlexNet Code Insight as a <i>Reviewer</i> .
	2. Click the My Project button.
	3. To select a project to review pending requests, click the magnifying glass icon. The <b>Project</b> page appears.

4. Click the **Requests** tab. A list of requests appears.

Summary	Inventory Reque	sts	Tasks Policies Comm	ents					
Basic Searc	Advanced Search	Filter:	All Requests	~	Search:	Q			
ld 🖛	Requester	Comp	All Requests		nse	Review Deadline	Status	Reviewed By	Actions
15	Alex Rybak	VMw	Completed Requests		ptaculous 1.8.1 License	01/24/2012	Approved	Manual	D
10	Alex Rybak	itext (		200	J Affero General Public License v3.0	01/05/2012	Pending	Manual	0
8	Alex Rybak	proto	Requests Requiring My Action Associated Requests	on	license (also X11)	12/29/2011	Approved	Manual	
7	Alex Rybak	zlib (*	<sup>1</sup> Unassociated Requests		libpng License	12/26/2011	Pending	Manual	
6	Alex Rybak	Any (	Component (Any Version)	МП	license (also X11)	11/02/2011	Rejected	Manual	
5	Alex Rybak	Any (	Component (Any Version)	МП	license (also X11)	11/02/2011	Approved	Manual	

- 5. To sort this list, use the pull-down **Filter** menu. You can choose to view All Request, Completed Requests, My Submitted Requests, Requests Requiring My Action, Associated Requests, and Unassociated Requests. If you have Reviewer permissions, you will also see a Request filter for My Drafts.
- 6. To search for a component related to a request, enter a string in the Search field.

## **Resubmitting Requests**

FlexNet Code Insight provides the ability to resubmit the request for review after editing it or adding policy without involving the requester, so that it can be reviewed as quickly as possible in the most automated fashion.

The ability to resubmit requests is useful in the following situations:

- After the reviewer has edited and cleaned up the request: reviewers often make edits to the request and resubmit it for review. Some businesses have a process in place that prevents or discourages the requester from selecting a license for a requested component due to trust issues and potential for user error. The requesters must make a guess at selecting a license or select "I don't know" as the license value. During triage review, a dedicated reviewer performs the necessary research and adds the proper license. At this point, the reviewer can recall the request and resubmit it for review.
- When the request requires a policy review by the legal department: if the legal department adds a new policy to the system and wants to check one or more pending requests against this policy, a member of the legal department can submit the requests for review without involving the original requester.
- When the request requires a manual review: if the legal reviewer wants to return the request to triage review for additional information, the reviewer can resubmit the request so it can go to triage without involving the original requester.



#### To resubmit a request, do the following:

- 1. Log into FlexNet Code Insight.
- 2. Click My Project.
- 3. Click the magnifying glass icon. The **Project** page appears.
- 4. Click the Requests tab. A list of requests appears.
- 5. Select the request you want to resubmit and click **Resubmit**. The selected request will be recalled and submitted for review.

#### Chapter 11 Reviewing Pending Requests

Resubmitting Requests

# **Copying & Branching Projects**

This section contains the following topics:

- Introduction to Project Copy Feature
- Copy Type: Project Configuration Only
- About Concurrently Open Workspaces

# **Introduction to Project Copy Feature**

This feature allows project owners to copy a project as follows:

- Project Configuration Only
- Custom Project Copy: This option enables the Custom Project Copy tab, which offers many options for customizing your project copy operation.
- Complete Project Copy

You can use the complete project copy operation or use a project as a template to create a new project by using the custom project or project configuration copy operation.

The two main purposes of the project copy feature are to support the following scenarios:

- Reduce the administrative effort for multiple projects with similar options, users, and workflow configuration.
- Facilitate a branching scenario to mirror what is happening to the scanned codebase.

### **Copying a Project to Reduce Administration Effort**

You can copy an existing project's settings to create a new project and in turn significantly reduce the administrative effort of re-defining all of the project settings including user provisioning and workflow definitions. For example:

• Project ePortal represents your FlexNet Code Insight Portal product.

- FlexNet Code Insight Manager, represented by project eManager, is developed by the same engineering team and has the same users and workflow definition as the FlexNet Code Insight Portal product.
- Since the development team is large with hundreds of users, it's practical to copy the project settings from ePortal to eManager. Once the copy is completed, any necessary changes can be made to the new project. This process is much simpler than configuring the new project from scratch. It can be accomplished by copying project ePortal to a new target project eManager using the Type option "Project Configuration Only".

### Copying a Project to Support Branching a Codebase

If a codebase is branched, the audit work needs to also be branched so that independent auditing results can be available for both codebases. Therefore, project data must be copied for the purposes of branching an audit.

The basic scenario is as follows:

- Project ePortal represents your FlexNet Code Insight Portal product.
- The current release of ePortal is 1.2. This codebase has undergone some level of auditing and contains inventory, requests, and other data to represent the audit work and results.
- Development needs to begin on version 1.3 of ePortal.
- The codebase is branched, and now there is a codebase for the ePortal 1.2 and ePortal 1.3 product.
- Project "ePortal 1.2" needs to be copied to project "ePortal 1.3".
- The project owner for ePortal 1.2 can make a copy of the project, call it "ePortal 1.3," and map the codebase from the source project to the target project. As long as the corresponding file exists in the target project, all associated scan results and audit data are be copied to the target project.
- Along with the scan results and audit data, all existing inventory items, requests, and other source project data are also copied to the target project.
- Once the copy operation completes, the two projects are considered to be independent and any changes made to either project does not impact the other project.

## **Copy Type: Project Configuration Only**

Project owners are the only ones with permission to copy projects. The following are the copy options available on the pulldown menu:

- Project Configuration Only
- Custom Project Copy
- Complete Project Copy

To copy a project configuration only, do the following:

- 1. Log into FlexNet Code Insight as an **Owner**.
- 2. Click the Projects button on the Main menu. The My Projects page appears.

Task

3. Select a project from the list and click the **Project Copy** icon () associated with that project. The **Project Copy** page appears:

📁 Project Copy		
General Options Custom	Copy Options Workspace Options	
Project Copy Type	Project Configuration Only	
Source Project	ePortal 1.3	
Target Project		

The default copy command in the **Project Copy Type** pull-down menu is **Project Configuration only**.

- 4. Enter a name for the new project in the Target Project field.
- 5. Click the Copy Project button.

## Data Copied During Project Configuration Copy Operation

This section explains what data are copied during a project configuration copy.

### **Project Settings: Workflow**

- Name is provided by the source project owner during the invocation of the project copy.
- Description is the same in the source project; the project owner can update this after the copy operation completes.
- Team is provided by the source project owner during the invocation of the project copy.
- Owner is the same as the source project; the project owner can update this after the copy operation completes.
- Project Summary Email Frequency is the same as the source project; the project owner can update this after the copy operation completes.
- Request Review Reminder Email Frequency is the same as the source project; the project owner can update this after the copy operation completes.
- Enable Inventory Quick Review is the same as the source project; the project owner can update this after the copy operation completes.
- Auto-Publish System-Detected Inventory is the same as the source project; the project owner can update this after the copy operation completes.
- Apply Policies to Inventory is the same as the source project; the project owner can update this after the copy operation completes.
- Request Form is the same as the source project; the project owner can update this after the copy operation completes.
- Review Levels are the same as the source project; the project owner can update these after the copy operation completes.

- Users—Observers are the same as the source project; the project owner can update these after the copy operation completes.
- Users—Auditors are the same as the source project; the project owner can update these after copy operation completes.
- Users—Security Analysts are the same as the source project; the project owner can update this after the copy operation completes.
- Users—Requesters are the same as the source project; the project owner can update this after the copy operation completes.
- Users—Reviewers are the same as the source project; the project owner can update these after the copy operation completes.

### Copy Type: Custom Project Copy

Project owners are the only ones with permission to copy projects.

- 1. Log into FlexNet Code Insight as an **Owner**.
- 2. Click the My Project button on the Main menu.
- **3.** Select a project from the list and click the **Project Copy** icon () associated with that project. The **Project Copy** page appears.

	Policies Scheduler 3 Research 2 Reports	Welcome Owner   🏭 My Settings   🛟 Help   🖏 Logoi
Project Copy		
General Options Custom	Copy Options Workspace Options	
Project Copy Type	Custom Project Copy	
Source Project	Project Configuration Only	
<ul> <li>Target Project</li> </ul>	Custom Project Copy	
	Complete Project Copy	

- 4. Select **Custom Project Copy** from the pull-down menu. This enables the Custom Copy Optionstab.
- 5. Select the Custom Copy Options tab.

General Options	Custom Copy Options	Workspace Options		
Copy Works	spaces			
Select Worl	kspaces to Copy	▼ ePortal_1_3		
Mark all Fil	es as Unreviewed			
Recall all P	ublished Groups			
Copy Inven	tory			
Inventory Review Status		Leave As-Is	~	
Copy Reque	ests			
Request Review Status		Leave As-Is	~	
Copy Polici	es			
Copy Proje	ct Comments			
Copy Metadata				

On the **Custom Copy Options** tab the following checkboxes are checked by default:

- Copy Workspaces
- Select Workspaces to Copy
- Copy Inventory
- Copy Requests
- Copy Policies
- Copy Project Comments
- Copy Metadata

The **Inventory Review Status** and **Request Review Status** pull-down menus are set to Leave-As-Is by default. You can change the defaults to any combination of Reset to Ready for Review and Reset to Draft.

6. Click the Copy Project button.

### **Copy Type: Complete Project**

Project owners are the only ones with permission to copy projects.

- 1. Log into FlexNet Code Insight as an **Owner**.
- 2. Click the My Projects button on the Main menu.
- 3. Select a project from the list and click on the **Project Copy** icon () associated with that project. The **Project Copy** page appears.

Workspace Options	
nplete Project Copy	
ect Configuration Only	
com Project Copy	
	plete Project Copy

4. Select Complete Project Copy from the Project Copy Type pull-down menu. The Workspace Options tab appears:

Project Copy					
General Options Cust	om Copy Options Workspace Options				
Pre-Copy Options	Compare Source and Target File Paths (only files that are marked as reviewed, tagged, or associated with groups will be compared)				
Workspace #1	Workspace Name				
	Source: ePortal_1_3				
	Target:				
	Workspace Software Configuration Management Settings				
	Source:				
	Git URL:	https://github.com/copton/reversi.git			
	Git Update To:	Latest Revision			
	SCM Destination Folder:	C:\Cleanroom\git_repo\			
	Target:				
	Git URL:	http:// <server>/<path_to>/<repository>.git;</repository></path_to></server>			
	Git Update To:	Latest Revision			
	SCM Destination Folder:	Browse Type			
	Workspace Folders to Scan				
	Source: C:\Cleanroom\git_r	epo\reversi\			
	Target:	Browse Type			

- 5. In the Workspace Name section, enter a name in the Target field.
- 6. In the Workspace Folders to Scan section, click on the Browse or Type button:
  - The **Browse** button opens a file system tree for the scan server on which you are working.
  - The **Type** button opens a dialog where you can enter the name of the input scan folder you wish to use.
- 7. On the **Workspace Options** tab, the Compare Source and Target File Paths checkbox is checked by default. Only files marked as reviewed, tagged, or associated with groups will be compared. Files that have not had any of these operations performed on them are not compared by the pre-copy analysis operation. This pre-copy codebase comparison lets you:
  - Know which files from the source codebase are not present in the target codebase: This means that files were removed after the codebase branching operation was performed.

- Know which target files are different from the source with the same relative path: This means that the target files were modified after the codebase branching operation was performed.
- Address file issues before the actual project copy, if appropriate.

## Data Copied During the Copy Operation

This section explains which data is copied during the complete project copy.

#### **Project Settings: Workflow**

- Name is provided by the source project owner during the invocation of the project copy.
- Description is the same as the source project; the project owner can update this after the copy operation completes.
- Team is provided by the source project owner during the invocation of the project copy.
- Owner is the same as the source project; the project owner can update this after the copy operation completes.
- Project Summary Email Frequency is the same as the source project; the project owner can update this after the copy operation completes.
- Request Review Reminder Email Frequency is the same as the source project; the project owner can update this after the copy operation completes.
- Enable Inventory Quick Review is the same as the source project; the project owner can update this after the copy operation completes.
- Auto-Publish System-Detected Inventory is the same as the source project; the project owner can update this after the copy operation completes.
- Apply Policies to Inventory is the same as the source project; the project owner can update this after the copy operation completes.
- Request Form is the same as the source project; the project owner can update this after the copy operation completes.
- Review Levels are the same as the source project; the project owner can update these after the copy operation completes.
- Users—Observers are the same as the source project; the project owner can update these after the copy operation completes.
- Users—Auditors are the same as the source project; the project owner can update these after the copy operation completes.
- Users—Security Analysts are the same as the source project; the project owner canupdate these after the copy operation completes.
- Users—Requesters are the same as the source project; the project owner can update these after the copy operation completes.
- Users—Reviewers are the same as the source project; the project owner can update these after the copy operation completes.

#### Workspace Settings: General

- Name is provided by the source project owner during the invocation of the project copy.
- Description is the same as in source workspace; the project owner or auditor can update this after the copy operation completes.
- Folders to Scan are the same as the source workspace, and they are updated with the new Target Scan Paths that are provided by the source project owner during the invocation of the project copy.
- Excluded File Patterns are the same as the source workspace; the project owner or auditor can update these after the copy operation completes.
- Enable Incremental Scanning is the same as the source workspace; the project owner or auditor can update this after the copy operation completes.

#### **Workspace Settings: Detection**

• All options are the same as the source workspace; the project owner or auditor can update these after the copy operation completes.

#### **Workspace Settings: Source Code Options**

• All of the CodeRank<sup>™</sup> attributes sliders are the same as the source workspace; the project owner or auditor can update these after the copy operation completes.

#### Workspace Settings: Automated Analysis

• All options are the same as the source workspace; the project owner or auditor can update these after the copy operation completes.

#### Workspace Settings: Software Configuration Management (SCM)

• The SCM settings from the source workspace are shown and can be updated and applied to the target workspace.

#### Workspace Reports

• The workspace reports are not copied as part of the project copy operation. These reports can be generated after the target workspace scan completes, so the report data represents the target codebase and scan results.

#### **File Tags**

- Tag data is copied, and file paths are updated to reflect the target codebase.
- If a file with the same relative path existed in the source codebase, but is not present in the target codebase, its tag assignments are not copied over.

• A new tag "File Changed Since Workspace Copy" is applied to all files which have the same relative file path in the target codebase, but whose MD5 is different from the source codebase. This allows the project owner or auditor to review the file and determine whether additional auditing work is required due to the changes in that file. Furthermore, if the source file was marked as reviewed, then that tag assignment is removed (since this file has changed since the workspace copy).

#### Groups

- Group data is copied and file paths are updated to reflect the target codebase.
- Groups with zero files are recalled, but the group is not deleted from the project. Users can either add files to the empty group and re-publish (all existing inventory item data are retained from the source inventory item), or delete the group.

#### Inventory

- Inventory items from the source project are copied to the target project with all data preserved as-is, except for the associated project ID.
- The review status from the source inventory item is maintained in the target inventory item in the target project.
- All comments associated with the source inventory item are copied to the target inventory item in the target project with the original posted on and posted by values.
- All questions and associated answers associated with the source inventory item are copied to the target inventory item in the target project with the original posted on, posted by, answered on, and answered by values.
- All checklist items associated with the source inventory item are copied to the target inventory item in the target project with the original posted on and posted by values, as well as completed on and completed by, if the checklist items were marked as completed.
- All attachments associated with the source inventory item are copied to the target inventory item in the target project with the original uploaded on and uploaded by values.

#### Requests

- All of the requests from the source project are copied as-is to the target project with the exception of updating the project ID to the target project value. All of the original dates (created on, submitted on, reviewed on, etc.) from the source request are retained in the target request.
- Draft Requests are copied to the target project as an un-submitted draft request.
- Pending Requests are copied to the target project as a pending request. Any approvals that are already made as part of the completed portion of the request review workflow are preserved in the target project. All reviewers that have yet to take action on the pending request need to review it both in the source project as well as the target project.
- Completed requests are copied to the target project as completed request and retain thesame IP review status and security review status as that of the source request.

#### **Tasks**

• All of the tasks from the source project are copied as-is to the target project with the exception of updating the project ID to the target project value. All of the original dates (for example, created on, completed on) from the source task are retained in the target task.

#### **Policies**

• Any policies with the source project explicitly selected as part of the scope via the **Project** selection widget are updated to include the target project as well. This does not apply to policies with a global or team scope, because the target project is already included as part of the team or global policy.

#### Comments

All project comments are copied with their original created by and created on values.

## **Pre-Copy Operations**

To reduce the risk of failure of the project copy operation, check the following before starting the copy process:

- Whether target workspace names provided by the project owner already exist on the scan server.
- Whether each scan server is reachable.
- Whether there is enough disk space remaining on the scan server for the workspace copy operation.
- The scan server scheduler queue to ensure that there are no active or scheduled tasks for any source workspaces.
- Whether there are any workspaces which are blocked by a project owner or auditor modifying the workspace settings.
- Whether there are any workspaces that are opened by the project owner or auditor in Detector.
- Ensure that target paths across all workspaces in a project for which an auditor has used the file (applied a tag, added to a group, or marked as reviewed). To determine inconsistencies, perform the following actions:
  - Create a list of all file paths that are no longer present in new project codebase but were in the source codebase
  - Create a list of all file paths that are same relative path but different MD5 from the source codebase

Provide a file paths comparison summary before proceeding with the project copy, and allow users to cancel the copy if they choose.

## Blocking Access to Source & Target Projects During Copy Operations

Access to the source project, target project, and associated workspaces needs to be blocked during the duration of the project copy operation. This includes web UI, Detector, and ScriptRunner API access.

#### **Post-Copy Scan**

All workspaces are scheduled for a full scan after the project copy completes to ensure that the scan results are accurate for the target codebase.

## **Email Notification**

The project owner who invoked the project copy is notified by email when the copy operation has completed. At that point, the source and target project are available for use.

## **Target Project Cleanup Options after Copy**

Once the project copy operation completes, there are several manual steps required to ensure that the target project accurately reflects the target codebase. The following list of tasks should be considered by the project owner, auditors, requesters, reviewers, security analysts, and policy administrators:

- Review and update (if necessary) the target project settings.
- Review and update (if necessary) the target workspace(s) settings.
- Software Configuration Management (SCM) options are not included in the project copy, so these properties needs to be set if the target workspaces are to be associated with a codebase managed via an SCM tool.
- If any workspace settings are changed, consider re-scanning the workspace to ensure that the scan results accurately reflect the target codebase.
- Run any necessary workspace reports so that the target codebase is properly reflected in the report contents.
- Review the scan results in Detector after the post project copy workspace scan(s) completes.
- Use the new tag "File Changed Since Workspace Copy" as a filter to review any files that have the same relative file path in the source and target codebase, but with file content that has changed. These files may have been altered by the SCM tool as part of the branching operation, or these files have actually undergone content changes via human editing. In any case, it is best for the auditor to review these files.
- Review any groups with zero (0) files. These are groups that have no files with thesame relative path between the source and target codebase.
- Files may have moved around in the target codebase, and these files need to manually be added back into existing groups.
- Files may have been intentionally deleted, and the group may be deleted as well, since the inventory is no longer present in the target codebase.
- Review the list of inventory items, and ensure that they have the proper review status.
- Complete all pending reviews for items undergoing a full review. Reviewers need to review the same inventory items in both the source and target projects.
- Review any policies whose scope has been explicitly altered to include the target project. If the policies do not apply, manually adjust the policy scope.

## **About Concurrently Open Workspaces**

Because project copying (custom and complete) requires opening workspaces, it is possible that if there are a large number of workspaces in a given project that project copy may fail. By default, the maximum allowable open workspaces on a given scan server is 50. Increase the dispatcher.maxNumberOfOpenedWorkspaces property in the scanEngine.properties file to allow more workspaces to be open at a given time. You will need to restart the Tomcat server for this change to take effect.



# **Reviewing Vulnerabilities**

This section provides the procedure for doing a security scan by reviewing vulnerabilities. The section contains the following topics:

• Vulnerabilities

## **Vulnerabilities**

When an inventory item is scheduled for a full review by a project owner and it has been through a review and reconciliation process to determine its IP compliance state, a secondary review by the security analyst assigned to the project must occur if the inventory item contains associated security vulnerabilities.

Task	To review vulnerabilities, do the following:
	<b>1.</b> Log into FlexNet Code Insight as a <i>Security Analyst</i> . A security analyst is a user with a project participant role who is assigned as a security analyst for a given project.

- 2. Click the **My Projects** button, and a list of projects opens.
- 3. Click the magnifying glass icon next to the project you want to review. The Project page opens.
- 4. Click the Inventory tab.

ePort	al 1.3											
Summar	y Workspaces Inve	entory Requests	asks Policies Comments									
Basic S	earch Advanced Search	Filter: All Inventory Iten	s Search:								P	
d <del>.</del>	Name	Component	License	# Files	412	*			9	Priority	Review Status	Acti
2025	mcrypt 2.6.8	mcrypt 2.6.8	GNU General Public License v3.0	1			-			2 - High	Ready for Review	
10	scriptaculous 1.8.1 scriptaculous 1.8.1 scriptaculous 1.8.1 License 6	scriptaculous 1.8.1 License		1					4 - Low	Approved		
9	Text 5.1.2	itext 5.1.2	GNU Affero General Public License v3.0	1	1					2 - High	Pending Review	
3	libpng 1.0.6	libpng 1.0.6	zlib/libpng License	1	1.75		1	26		6 - Not Set	Needs More Informat	
5	prototype 1.6.0.2	prototype 1.6.0.2	MIT license (also X11)	1				-	1.00	6 - Not Set	Approved	
1	zlib 1.2.2	zlib 1.2.2	zlib/libpng License	1	170	1		2		6 - Not Set	Rejected	
3	zlib 1.2.1	zlib 1.2.1	zlib/libpng License	1		1		2	( <b>*</b> )	6 - Not Set	Pending Review	
2	zlib 1.1.3	zlib 1.1.3 zlib 1.1.3 zlib/libpng License	lib 1.1.3 zlib 1.1.3 zlib/libpng License 1 -		12		1	653	6 - Not Set	Rejected	<u>a</u>	
1	zlib 1.2.3	zlib 1.2.3	zlib/libpng License	4	-		-		-	6 - Not Set	Approved	

- 5. Select an inventory item, and click the associated magnifying glass icon. The Inventory details page appears.
- 6. In the **Components** line, click the **Vulnerability Shield** icon (**V**) in the top left corner of the **Inventory Details page** to view vulnerabilities details. The **Contains the Following Security Vulnerabilities** dialog appears:

				🔂 Add New Vulnerabilit
	Score *	Severity	Name	Description
Ð	10	HIGH	CVE-2004-0597 🗗	Multiple buffer overflows in libpng 1.2.5 and earlie
Ð	7.8	HIGH	CVE-2010-0205 🗗	The png_decompress_chunk function in pngrutil.c in I
Ð	7.5	HIGH	CVE-2010-1205 🗗	Buffer overflow in pngpread.c in libpng before 1.2.4
Ð	7.5	HIGH	CVE-2002-1363	Portable Network Graphics (PNG) library libpng 1.2.5
Ð	7.5	HIGH	CVE-2008-1382	libpng 1.0.6 through 1.0.32, 1.2.0 through 1.2.26, a
Ð	7.5	HIGH	CVE-2006-3334 🚱	Buffer overflow in the png_decompress_chunk function
Ð	6.8	MEDIUM	CVE-2009-0040 🚱	The PNG reference library (aka libpng) before 1.0.43
Ð	6.8	MEDIUM	CVE-2011-2690 🗗	Buffer overflow in libpng 1.0.x before 1.0.55, 1.2.x
Ð	5	MEDIUM	CVE-2007-2445 🛃	The png_handle_tRNS function in pngrutil.c in libpng
Ð	5	MEDIUM	CVE-2009-5063 🚱	Memory leak in pngwutil.c in libpng before 1.2.39bet
Ð	5	MEDIUM	CVE-2004-0421 🚱	The Portable Network Graphics library (libpng) 1.0.1
Ð	5	MEDIUM	CVE-2006-7244 🚱	Memory leak in pngwutil.c in libpng 1.2.13beta1, and
Ð	5	MEDIUM	CVE-2010-2249 🗗	Memory leak in pngrutil.c in libpng before 1.2.44, a
ŧ	5	MEDIUM	CVE-2011-2691 🗗	The png_err function in pngerror.c in libpng 1.0.x b
	5	MEDILIM	CVE 2004 0500 -51	Multiple integer overflowe in the (1) ppg, read, ppg i

- 7. To expand the descriptions, click the **Plus** icon to the left of the **Score** column.
- 8. Click the CVE links to read information about each vulnerability in the National Vulnerability Database.
- **9.** From the **Change Inventory Status** pull-down menu, select **Approve**, **Reject** or **Schedule Full Review** of the inventory item when you have completed reviewing the associated vulnerabilities.
- **10.** If action is required based on the vulnerability review, create security checklist items for the inventory item to track this work. For more information, visit https://flexeracommunity.force.com/customer/CCContactSupport.



# Metadata Framework

This section contains the following topics:

- Metadata
- Administering Metadata Sections and Fields

## Metadata

FlexNet Code Insight contains a flexible metadata framework to allow support of additional information associated with all FlexNet Code Insight-managed entities. This, in turn, makes the system more valuable as a repository for your code. Metadata support is provided via the Web UI as well as via public APIs using ScriptRunner.

## **Administering Metadata Sections and Fields**

Task

To administer metadata sections and fields for FlexNet Code Insight-managed entities via the Web UI, do the following:

- 1. Log into FlexNet Code Insight as **Application Administrator**. Only a user with the Application Administrator permission can manage metadata sections and fields.
- 2. Click the Administration button on the Main menu, and select Metadata from the pull-down menu:

🕤 Home 🛛	Administration •	- Welcome Admin   🧞 My Settings   🐉 Help   🦏 I
Mome	💩 Users 🍓 Teams	
Welcome Ac	Projects	t login was on 04/12/2012 15:59.
🚖 My Sł	0 Metadata	
• Create	Import	
Create :	E Scripting	
Create :	🚱 Updates	

The Metadata Field Administration page opens to Team. In this example, click on the Project tab:

Home   🎲 Adminis	tration •							Welco	ome Admin 🛛 🏭 My Se	ettings	🤣 Help 🛛	- Logo
Metadata Field A	dministra	ation										
eam Project	Group	Component	Version	License	Inventory	Request	Policy					
									0	Add Proje	ct Metada	ta Section
Name				Descriptio	in						Actio	ins
Uncategorized												
Search:			P					C	Add Pro	oject Metad	lata Field	
Name		Disp	lay Name					Input Type	Hidden		Actio	ns
Build Name		Build	Name					Single Line Text	Yes	4	2	3
Build Number Build Number						Single Line Text	Yes	<b>1</b>	B.	3		
CertificationLevel Color CertificationLevel		l Color				Single Line Text	Yes	<b>1</b>	B.	3		
CertificationLevel Id CertificationLevel			el Id				Single Line Text	Yes	<b>1</b>	B.	3	
CertificationLevel Na	me	Cert	ficationLeve	I Name				Single Line Text	Yes	<b>1</b>	B.	3
CompilerTarget Id		Com	pilerTarget lo	t				Single Line Text	Yes	<b>1</b>	R (	3
CompilerTarget Name		Com	pilerTarget N	lame				Single Line Text	Yes	<b>1</b>	R	3
CPM Data CPM Data							EntityRef	Yes	<b>1</b>	R (	3	
Filter Date		Filter	Date					Single Line Text	Yes	<b>1</b>	R	3
Format Id		Form	nat Id					Single Line Text	Yes	合县	R (	3

The following FlexNet Code Insight-managed entities can support associated metadata fields organized into the metadata sections:

- Team
- Project
- Group
- Component
- Version
- License
- Inventory
- Request
- Policy

Metadata fields are organized into metadata sections for a given entity to allow for a logical grouping of related data. The Metadata Field Administration page is comprised of tabbed types of metadata and each tabbed page is split into two sections as shown in Figure 88.

The top portion of the page allows for management of metadata sections for FlexNet Code Insight-managed entities. A metadata section definition consists of a name and description. Once metadata sections are defined, they can be ordered as desired by clicking on the **up** and **down** arrows in the metadata sections table.

## **Adding a Metadata Section**

#### To add a metadata section, do the following:

- **1.** Log into FlexNet Code Insight with **Application Administrator** permissions. Only a user with the Application Administrator permission is allowed to manage metadata sections and fields.
- 2. Click the Administration button on the Main menu, and select Metadata from the pull-down menu.
- Click on the tab for the type of Metadata to which you wish to add a section. In this example, select the Project tab.
- Click on the green Plus icon Add Metadata Section button.
- 3. The Add Metadata Section dialog box appears:

Name	
Description	

4. Complete the Name and Description fields.



**Note** • A section name is unique to an entity.

5. Click the Save button.

## Adding a Metadata Field

The bottom portion of the **Metadata Field Administration tab** allows you to manage metadata fields for a given metadata section. A metadata field definition consists of a Name, Display Name, Help Text, Input Type, Section, and a Hidden Option. Once metadata fields are defined, they can be ordered as desired within their metadata section by clicking on the **up** and **down** arrows in the metadata fieldstable.

# Task

Task

#### To create a metadata field, do as follows:

- 1. Log in to the system with application administrator permissions. Only a user with the Application Administrator permission is allowed to manage metadata sections and fields.
- 2. Select Administration from the Main menu, and select Metadata from the pull-down menu.
- 3. Click the tab for the type of Metadata to which you wish to add a section. In this example, select the Project tab.
- 4. Click the Plus icon Add Metadata Field button. The Add Metadata Field dialog appears.

Name		
Display Name		
Help Text		
Input Type		~
Input Type Section	Uncategorized	~

- 5. Complete the fields on the Add Metadata Field dialog:
  - Name: This is a unique identifier for the metadata field for a given entity. This is a required field.
  - Display Name: This is the label that shows up in the Web UI when displaying or assigning the metadata field value. This is a required field.
  - Help Text: If a value is entered here, a help icon will be shown next to the metadata field when displaying or assigning the metadata field value. This is an optional field.
  - Input Type: The input type will determine which validations need to occur when assigning a metadata value for the field as well as how to display the assigned value. The following input types are supported.
  - Date
  - Numbers
  - Integer (Whole Number)
  - Number with Decimal
  - Text Types
  - Single Line Text
  - Short Multiple Line Text
  - Long Multiple Line Text (over 4,000 characters)
  - URL
  - Yes/No
  - Section: The section to which this metadata field belongs. This value may be edited once the metadata field is defined. During the initial metadata field definition, the value is set to the metadata section for which the metadata field was created.
  - Hidden: If selected, this metadata field will not be shown in the Web UI, but is still accessible via public APIs. This is intended to be used for cases where a metadata field for a given entity needs to store data that should not be viewable or editable via the Web UI.
- 6. Click Save.

Metadata field administration is also supported via the public APIs.

Note • Any metadata field defined without a selected section will be located in the Uncategorized tab in the Web UI.

The imported metadata fields can then be edited in the Web UI to organize them into the desired section. The process of defining metadata fields via the public APIs uses an XML file to define the metadata fields and a groovy script to import the data. Refer to the sample file (sample-license- metadata-definitions.xml) located in the / scriptRunner/scripts directory.

## Viewing, Editing, and Assigning Metadata Values

Web UI access to metadata fields for viewing and assigning values is limited to the following entities:

- Projects via the **Project Summary** page.
- Inventory items via the **Inventory Details** page.
- Requests via the Request Details page (Additional Info tab).
- Components via the research, inventory details, and request details pages.
- Component versions via the research, inventory details, and request detailspages.
- Licenses via the research, inventory details, and request details pages.

Task	To view, edit and assign metadata values associated with an inventory item via the Web UI, do as follows:

- 1. Log into FlexNet Code Insight as an **Application Administrator**. Only a user with **Application Administrator** permission is allowed to manage metadata sections and fields.
- 2. Click the Administration button on the Main menu, and select Metadata from the pull-down menu:

🕤 Home	Administration •		Welcome Admin   🌄 My Settings   🤣 Help   🐗 Logout
Home Welcome A	Cams Teams	login was on 04/12/2012 15:59.	
🚖 My Sl	Metadata		
<ul><li>▶ Create</li><li>▶ Create</li></ul>	<ul> <li>Import</li> <li>Scripting</li> <li>Updates</li> </ul>		

- 3. Click the tab for the type of Metadata to which you wish to add a section. In this example, select the **Project** tab.
- 4. Select an entity and click the **Pen and Paper** icon to view the metadata associated with that entity instance. The **Edit Metadata** dialog opens for that instance.

Name	Build Number	
Display Name	Build Number	
Help Text		
	E	
Input Type	Single Line Text	~
	Uncategorized	~
Section	oncacegonzed	

Another way to view metadata is to log into FlexNet Code Insight as a user without administrator privileges. For example, log in as **Owner**.

- 5. Click the My Projects button on the Main menu.
- 6. Select the Magnifying glass icon associated with the project inventory you wish to view.
- 7. Select the Inventory tab.
- 8. Select an inventory item and click one of the following icons:
  - Click the view component Metadata icon (<sup>1)</sup>) in the **Component** field at the top of the page.
  - Click the License Details icon (<sup>1</sup>) next to the license name in the **Component** field at the top of the page or in the **Possible Licenses** section.
  - Click the View Inventory Metadata button (<u>View Inventory Metadata</u>) in the Inventory Details page Inventory Metadata section.
- 9. Click the View Inventory Metadata button. The Metadata information opens in View mode.
- **10.** Click the **Edit** button at the bottom of the **Metadata** dialog, and the metadata information appears in Edit mode.

Disclosures		
Requires Source Distribution	Yes 💌	
Disclosure - Notices	Mcrypt is a simple encryption program, intended to be replacement for the old unix crypt(1). Look at COPYING for license information and the individual files for more information_COPYING enclase only for the monort program and not the	•
Disclosures - Copyright Statements	The principal author and maintainer of mcrypt is Nikos Mavroyanopoulos <nmav@gnutis.org> Convribit balder in the monet preserve area</nmav@gnutis.org>	•
liscellaneous		
Deployed Associated Request Link	Yes	

=

**Note** • Use of the **Edit** button is restricted to those users allowed to edit metadata values.)

Metadata fields are displayed in sections as defined by a user with Administrator permissions. If there is Help Text for a given **Metadata** field, a **Help Text** icon appears. You can hovered over or click on the Help Text to display it.

11. Modify the values in the Metadata fields, and click the Save button to saveyour changes.

**Note** • Access to Metadata Field values and assignment of values for Metadata fields is also supported via the public APIs.

#### Using Public APIs to Access & Assign Metadata Field Values

Access to Metadata Field values and assignment of values for Metadata fields is also supported via the public APIs. The process of assigning Metadata Field values for FlexNet Code Insight-managed entity instances via the public APIs uses a CSV (comma-separated) values file format to specify the Metadata Field values for an entity instance, and a groovy script to import the data.

For more information, see the sample file (sample-license-metadata.csv) located in the /scriptRunner/scripts directory.

Chapter 14 Metadata Framework

Administering Metadata Sections and Fields



# **Using the Product Catalog**

This section discusses the Product Catalog and how to use it. The section contains the following:

• The Product Catalog

## **The Product Catalog**

FlexNet Code Insight provides the Product Catalog so your company's offering (products and services) can be represented in a hierarchy within FlexNet Code Insight. Once the Product Catalog items are in the system, they may be associated to requests and used to generate Third-Party Notices and other reports. The following use cases are applicable to the Product Catalog.

#### Associating Requests to Product Catalog Items

A FlexNet Code Insight user would like to file a request to use an OSS component and associate it to one or more versions of the product (i.e. ePortal 1.3, 1.4, 1.5) during or after request approval. With the product versions listed as items in the Product Catalog, the user can create the request from any project (including a non-audit Request project) and associate the request to one or more versions of the product Vatalog at any given any time. The user can also report on the request data and third party notices associated with the requests filtered by Product Catalog items. For more information, see Associating Product Catalog Items with a Request.

## **Associating Inventory with Requests Across Projects**

A FlexNet Code Insight reviewer would like to be able to associate an inventory item for zlib 1.2.3 to a request in another project (i.e. a Request Project) in order to determine its compliance state. This scenario can be achieved if both the project containing the inventory item and the request are associated to the same Product Catalog item.

## Generating Third-Party Notices for Requests based on Product Catalog Items

A FlexNet Code Insight legal user creates third-party notices for requests across multiple projects or a single global project. She would like to be able to generate a Third-Party Notices report for Requests based on her company's products and services. This can be done by associating the requests to the Product Catalog items and running the Third Party Notices Report for Requests (Filtered by Product Catalog).

## **Reporting on Findings Based on Product Catalog Items**

A FlexNet Code Insight user may want to limit the scope of a report based on Product Catalog data. FlexNet Code Insight currently offers the **Request Report (Filtered by Product Catalog)**.

## Administering the Product Catalog

The following attributes represent a Catalog item in FlexNet Code Insight:

- Name (required)
- URL (optional)
- **Description** (optional)
- Parent Item (optional)

The following functionality is currently available for Product Catalog:

- Create/Delete a catalog item.
- Place catalog item in the correct position in FlexNet Code Insight.
- Search for a catalog item across Projects/Requests.
- Associate a catalog item with an existing Project or existing Request.
- View associated Catalog items for a Project/Request.
- Report on all Requests associated with a Catalog item.
- Report on all Third-Party notices associated with a Catalogitem.

FlexNet Code Insight can be configured to display Product Catalog attributes. To modify how and where these attributes are displayed, modify the product.catalog.web.json file according to the steps below.

#### **Projects**

#### Task

To enable the Product Catalog feature for projects, do the following:

1. Open the .json file associated with your installation of FlexNet Code Insight:

<Code Insight\_ROOT>/config/core/product.catalog.web.json

2. Set the following property to "true" to enable the Product Catalog attribute on the **Project Details** page:

"project.details.product.catalog": { "enabled": true

As an alternative, set the property to "false" to disable the Product Catalog attribute from the **Project Details** page.

**3.** By default the Product Catalog attribute will appear on the Project Details page with a label "**Product Catalog**". To change the label text, modify the *entry.label.text* property:

"applyTo": ["project.details.product.catalog"],
"configuration": {
 "entry.label.text": "Product Catalog"

4. Be sure to restart the server after making modifications to the .json file.

#### **Requests**

Task	То е	enable the Product Catalog feature for Requests, do the following:
	1.	Open the .json file associated with your installation of FlexNet Code Insight:
		<code insight_root="">/config/core/product.catalog.web.json</code>
	2.	Set the following property to "true" to enable the Product Catalog attribute on the <b>Request</b> page:
		"request.details.product.catalog": { "enabled": true
	3.	Alternatively, set the above property to "false" to disable the Product Catalog attribute from the <b>Request Details</b> page.
	4.	By default the Product Catalog attribute will appear on the <b>Request Details</b> page with a label " <b>Product Catalog</b> ". To change the label text, modify the <i>entry.label.text</i> property:
		"applyTo": ["request.details.product.catalog"], "configuration": { "entry.required": false, "entry.label.text": "Product Catalog"
	5.	The following property determines where on the <b>Request Details</b> page the Product Catalog will appear:
		"insert.after": "_palamida_projectName"
	6.	Be sure to restart the server after making modifications to the .json file.

## **Adding Product Catalog Items**

You can create Product Catalog items in FlexNet Code Insight in the following ways:

• Import them using the **Import** option on the **Administration** pull-down menu.

(A) Towned	👌 User	s	
Import 🖞	🍓 Tean	ns	
Choose	🕼 Proje	cts	tems.xls Import
		uct Catalog	
1 Downlo 1 Downlo	Meta	data	or bulk license obligations import or bulk policy import
割 Downlo 割 Downlo	E Lega	I Templates	pr bulk request import pr bulk user import
≝ Downlo	🖺 Impo	rt	or bulk product catalog items import
	E Scrip	ting	
	💫 Upda		

• Add them manually using the **Create** option available after selecting **Product Catalog** from the **Administration** pull-down menu:

🔂 Home	🔅 Administration 🗸 👔	🕽 My Projects   🛃 Requests   🚦 Policies   🕑 Scheduler    Research   🕅 Reports	(?) Help
🕯 Import	👌 Users		
aport	🍓 Teams		
Choose	Projects	tems.xls Import	
	👶 Product Catalog		
Downlo  Downlo	Metadata	or bulk license obligations import or bulk policy import	
Downlo     Downlo	Legal Templates	or bulk request import or bulk user import	
Downlo	Import	or bulk product catalog items import	
	E Scripting		
	Updates		

## Viewing, Editing and Associating Product Catalog Items

Task

To edit a Product Catalog Item, do the following:

1. Select the item on the **Product Catalog Administration** page:

👌 Product Catalog Administrati	on		
			🔂 Create 📝 Edit 🔇 Delet
Name	Description	URL	
E Mobile 1.0	Mobile Application 1.0	http://www.mycompany.com/produ	cts/mobileapp-1.0 년
E Mobile 2.0	Mobile Application 2.0	http://www.mycompany.com/produ	cts/mobileapp-2.0 6
E Mobile 2.2	Mobile Application 2.2	http://www.mycompany.com/produ	cts/mobileapp-2.2
E Mobile 2.5	Mobile Application 2.5	http://www.mycompany.com/produ	cts/mobileapp-2.5 6
E Mobile 3.0	Mobile Application 3.0	http://www.mycompany.com/produ	cts/mobileapp-3.0 🗗
Mobile Applications	This is the parent catalog item for all Mobile Applications	http://www.mycompany.com/produ	cts/mobileapps 匠
😑 Operating System 1.0	Operating System 1.0	http://www.mycompany.com/produ	cts/os-1.0 🗗
\Xi Operating System 2.0	Operating System 2.0	http://www.mycompany.com/produ	cts/os-2.0 🚱
\Xi Operating System 3.0	Operating System 3.0	http://www.mycompany.com/produ	cts/os-3.0 🗗
Operating Systems	This is the parent catalog item for all Operating Systems	http://www.mycompany.com/produ	cts/os ලි

2. Click the Edit button. The Catalog Item dialog appears:

<ul> <li>Name</li> </ul>	Operating System 1.0	
URL	http://www.mycompany.com/products/os-1.0	
Description	Operating System 1.0	
Parent Item	Change Parent Clear Parent	

- 3. Modify the Catalog Item information:
  - Name
  - URL
  - Description
- **4.** To edit the hierarchy of a Product Catalog Item by changing the parent on the item, click the **Change Parent** button in the **Catalog Item** dialog and select a parent to assign to the item.



**Note** • A catalog item can have only one Parent catalog item at any given time. A Parent catalog item can have more than one child at any given time.

5. Click Save. Items that are parents are displayed with a folder icon in the Product Catalog Administration list:

🚡 Home   🎲 Administration 🕶   🌾	🛛 My Projects   🛃 Requests   🚦 Policies   🕑 Scheduler   🚯 Researc	h   22 Reports	(?) He
👌 Product Catalog Administrati	on		
			🕒 Create 📝 Edit 🙆 Dele
Name	Description	URL	
4 🚖 Mobile Applications	This is the parent catalog item for all Mobile Applications	http://www.mycompany.com/products/mobilea	pps 🚱
E Mobile 1.0	Mobile Application 1.0	http://www.mycompany.com/products/mobilea	pp-1.0 🗗
E Mobile 2.0	Mobile Application 2.0	http://www.mycompany.com/products/mobilea	pp-2.0 화
E Mobile 2.2	Mobile Application 2.2	http://www.mycompany.com/products/mobilea	pp-2.2 🗗
E Mobile 2.5	Mobile Application 2.5	http://www.mycompany.com/products/mobilea	pp-2.5 🗗
E Mobile 3.0	Mobile Application 3.0	http://www.mycompany.com/products/mobilea	pp-3.0 🗗
Operating System 1.0	Operating System 1.0	http://www.mycompany.com/products/os-1.0 g	P
Operating System 2.0	Operating System 2.0	http://www.mycompany.com/products/os-2.0 g	P
Operating System 3.0	Operating System 3.0	http://www.mycompany.com/products/os-3.0 g	P
Operating Systems	This is the parent catalog item for all Operating Systems	http://www.mycompany.com/products/os 🗗	

## Associating Product Catalog Items with a Project



To associate Product Catalog items with a FlexNet Code Insight Project, do the following:

- 1. Go to My Projects and click the Edit Project button for the project you want to edit.
- 2. On the Project Details page, click the Add Product Catalog button to display Product Catalog items.

😫 Project Details						
General Information Observers QuickReview Fac	cilitators Auditors Security Analysts					
* Name	adobe13	×				
Description		^				
		~				
* Team	reddi_team	×				
* Owner	Reddi Dakshnapu (reddi)	~				
Project Summary Email Frequency	Never	~				
Request Review Reminder Email Frequency	Never	~				
Project Form	None Selected	~				
Request Form	None Selected	~				
Advanced Options	<ul> <li>✓ Enable Inventory Quick Review</li> <li>✓ Auto-Publish System-Detected Inventory</li> <li>✓ Apply Policies to Inventory</li> </ul>					
Review Levels	Select a Request Form to enable the Review Levels options.					
Aliased Project	Add Aliased Project Remove Aliased Project					
Child Projects	Add Child Projects					
	Child Project 🛦					
* Scan Server	Scanner1	~				
Scan Root Path	D:\root\29	Browse Type Remove				
Product Catalog	Add Product Catalog Items Remove Product Catalog Items					
Product Type	None Selected	~				

3. Check the items that you would like to associate with the project and click **Select**:

	E conservation de la conservatio	Select All Clear
Name	Description	URL
🔲 🚍 Mobile Applications	This is the parent catalog item for all Mobile Applications	http://www.mycompany.com/products/mobile
Mobile 1.0	Mobile Application 1.0	http://www.mycompany.com/products/mobile
🕑 📃 Mobile 2.0	Mobile Application 2.0	http://www.mycompany.com/products/mobile
Mobile 2.2	Mobile Application 2.2	http://www.mycompany.com/products/mobile
E Mobile 2.5	Mobile Application 2.5	http://www.mycompany.com/products/mobile
Debile 3.0	Mobile Application 3.0	http://www.mycompany.com/products/mobile
🔲 \Xi Operating System 1.0	Operating System 1.0	http://www.mycompany.com/products/os-1.0 화
Derating System 2.0	Operating System 2.0	http://www.mycompany.com/products/os-2.0
Derating System 3.0	Operating System 3.0	http://www.mycompany.com/products/os-3.0 kg
Operating Systems	This is the parent catalog item for all Operating Systems	http://www.mycompany.com/products/os 🗗

## Associating Product Catalog Items with a Request

Task

To associate Product Catalog items with a FlexNet Code Insight Request, do the following:

- 1. Navigate to the **Request Details** page.
- 2. Click Add Product Catalog Items button to add product catalog items.
- 3. Click Remove Product Catalog Items button to remove catalog items.

Usage	Modifications	Encryption	Vault	Additional Information					
*	Component N	lame:							
	hibernate-hiber			Search Component V	iew Component Details	Clear Comp	onent		
	hibernate-hiberr	nate-orm (ic	1: 302846	) http://hibernate.org d	P				
	Hibernate's core	e Object/Re	lational N	1apping functionality					
*	Component V	ersion <sup>.</sup>							
	5.2.11		~	Add Version					
*	License Name								
•	GNU Lesser Ge		ic License	e v2.1	~	(?) Help E	Edit Possible Licenses	View License Details	
	Design to be						)		
*	Project Name								
	Team	reddi_t	eam						
	Project	adobe1							
	Burnelinet Control								
	Product Catal	-							
	Add Product Cata	alog Items	Remove P	roduct Catalog Items					
	Name			Description			URL		
	▷ 🗹 🧰 Mobile	Applications		This is the parent ca	atalog item for all Mobile A	pplications	http://www.mycompany.com/products/mobile		
		ng Systems		This is the parent ca	atalog item for all Operatir	ng Systems			
	E test								

4. Check the items that you would like to associate with the Request and click Select.

## Associating Inventory with Requests across Projects

To search for a request across multiple projects when associating inventory, the inventory item and request must share a **Product Catalog** item.

Task

To associate inventory with Requests across projects, do the following:

- 1. Associate the Product Catalog item with the given project.
- 2. Associate the Product Catalog item with the request.

	💋 My Projects   🗹 Requests   🚦 Policies   📎 Scheduler   🥹 Research   🔀 Reports	(?) H
General 1.3 Project → Inv	entory → zlib 1.2.3 (24 of 24 to be Reviewed)	
Component: zlib 1.2.3	💿 🏴 📀 🖨 🔰 🎔 Priority: 6 - Not Set 💉	Pending Review
License: zlib/libpng Licens	e 🗸 🕡 🏴 Remediation: Not Required	Change Inventory Status
		Reset to Ready for Review
Inventory Details This	d-Party Notice 🛛 🤿 Comments (1) 🛛 🤌 Questions (0) 🛛 🔔 Checklist Items (0) 🛛 📎 Attachments (0)	Create / Associate Request
Inventory Name	zlib 1.2.3	
Inventory Id	1	
Component Description	A free, lossless data compression lib for use on virtually any computer hardware and operating s across platforms. The compression method currently used in zlib never expands the data. Zlib's input data by more than a few bytes and can be reduced (at some cost in compression).	
Possible Licenses	zlib/libpng License 🕼 👩 🏴	Edit Possible Licenses List
As-Found License Text	View As-Found License Text	
Number of Files	3 inventory files (including files inside archives) View Inventory Files	
Review Status	Pending Review This inventory item is pending a complete IP review.	
Auditor Notes	None	
Detection Notes	Detection Confidence: 100% Supporting Evidence: Multi-Indicator: System rule 100052: MID-Rule for zlib 1,2,3 (Search Term	ms)

- 3. From the associated project, create an inventory item that matches the request component, version and license.
- 4. Schedule a Full Review for the inventory item and select the option to Associate the Request:

socia	ate Request						
d	Project	Requester	Component 🔺	License	Status	Action	ns
10	Request Project	Palamida User	zlib (1.2.3)	zlib/libpng License	Pending	<u>i</u>	3
ia a	Page 1 of	1	Show All			1	- 1 of

The request is available in the search results based on the Product Catalog association.

## Reporting on Requests (Filtered by Product Catalog)

The **Request Report (Filtered by Product Catalog)** option presents all request data associated with the selected catalog items.



1. Select Requests Report (Filtered by Product Catalog) from the Reports menu.

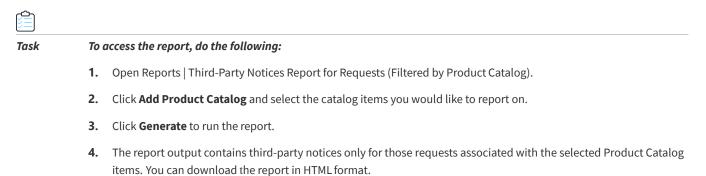
2. Click the Add Product Catalog button and select the catalog items you would like to report on. The report output contains the catalog items and their associated requests:

Requests Report (Filtere	d by l	Product Catalog)				Genera	ated on Monday, April 20,	2015 at 4:14 PM
								Download Report
There are 3 requests from 10 catalog	g items	Show / Hide					Ba Downlo	ad Excel Version
Name	De	escription			URL			
Mobile 1.0	M	obile Application 1.0			http://www.mycompany.com/produ	ucts/mobileapp-1.0		
Mobile 2.0	M	obile Application 2.0			http://www.mycompany.com/produ	ucts/mobileapp-2.0		
Mobile 2.2	M	obile Application 2.2			http://www.mycompany.com/produ	icts/mobileapp-2.2		
Mobile 2.5		obile Application 2.5			http://www.mycompany.com/produ	icts/mobileapp-2.5		
Mobile 3.0		Mobile Application 3.0			http://www.mycompany.com/products/mobileapp-3.0			
Mobile Applications	Th	This is the parent catalog item for all Mobile Applications			http://www.mycompany.com/products/mobileapps			
Operating System 1.0	Op	Operating System 1.0			http://www.mycompany.com/products/os-1.0			
Operating System 2.0	Op	Operating System 2.0			http://www.mycompany.com/products/os-2.0			
Operating System 3.0	Op	Operating System 3.0			http://www.mycompany.com/products/os-3.0			
Operating Systems	Th	This is the parent catalog item for all Operating Systems			http://www.mycompany.com/products/os			
Catalog Items	Reque	st Requester	Component	Version	License	Status	Request Type	Creation Date
Mobile 1.0 Mobile 2.0	<u>9 (URL</u>	.) Jane Doe	apache-jakarta-commons-codec	1.10	Apache License 2.0	Approved	Internal Use	04-07-2015
Operating System 1.0 Operating System 2.0 Operating System 3.0	<u>8 (URL</u>	.) <u>Jane Doe</u>	iquery	1.9	MIT License (also X11)	Created	Internal Use	03-25-2015
Operating System 1.0 Operating System 2.0 Operating System 3.0	Z (URL	.) Jane Doe	scriptaculous	1.9	MIT License (also X11)	Approved	Internal Use	03-25-2015

**3.** Click the **Show/Hide** button to display additional details for each catalog item attribute. HTML and Excel versions of the report are available for download.

# Reporting on Third-Party Notices for Requests (Filtered by Product Catalog)

The **Third-Party Notices Report for Requests (Filtered by Product Catalog)** option presents all third-party notice data for requests associated with the selected catalog items. To run this report, third-party notices should be created for requests.



#### Chapter 15 Using the Product Catalog

The Product Catalog



# **Performing Advanced Searches**

This section provides information about advanced searches:

- Advanced Searches
- Advanced Project Search Example

## **Advanced Searches**

FlexNet Code Insight contains an advanced search interface that allows parametric searches to be used for filtering the list of projects, inventory items within a project, components, and licenses.

Advanced search supports multiple search criteria that must all be met for an item to be returned. The search criteria consist of an entity, field, operator, and value. The list of available entities varies based on which entity is being searched as shown below:

## **Project Advanced Search**

- Project Description
- Project ID
- Project Name
- Project Owner
- Project Status
- Requester Name
- Project Metadata Fields
- Project Properties

## **Inventory Advanced Search**

- Inventory
- Request
- Component
- License
- Inventory Properties

## **Request Advanced Search**

- Request
- Inventory Fields
- Comment Text
- Has Comments
- ID
- Requester Name
- Review Deadline
- Status
- Component
- License
- Request Properties

## **Component Advanced Search**

These are components associated with project inventory.

- Component Properties
- Component Fields
- Description
- Has Encryption
- Has Vulnerabilities
- ID
- Is Custom
- Name
- Component Metadata Fields

## License Advanced Search

These are licenses associated with project inventory.

- Component
- License
- License properties
- License fields
- Comment Text
- Has Comments
- Has Family
- Has Obligations
- ID
- Is Custom
- Is Family
- Name
- Text
- License Metadata Fields

## Policy (Web UI) Advanced Search

Policy Properties

## Team (Web UI) Advanced Search

• Team Properties

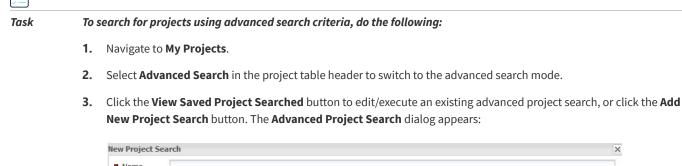
## Group (Detector) Advanced Search

Group Properties

## **Advanced Project Search Example**

To search for projects using advanced search criteria, perform the following steps.

þ



Name Description						
Criteria	Add New Project Search Crite					
	Entity	Field	Operator	Value	Actions	

4. Click the Add New Project Search Criteria button to define search criteria. The Project Search Criteria dialog appears.

Entity	Inventory	~
Field	Requires Source Distribution	~
Operator	=	~
Value	Yes	

- 5. Select and enter criteria for the search:
  - Select the entity to search by.
  - Select the entity field to search by.
  - Select the operator.
  - Select or enter the value for the entity field to search by.
- 6. Click Add.
- 7. Repeat as necessary to define other criteria for the search.
- 8. Click the **Save and Search** button or the **Search without Saving** button to invoke the search. To save the search without invoking it, click **Save**. The projects table is reloaded with all project records that match all the defined search criteria:

**Note** • When searching using the equals and not equals operator, only properties and/or metadata fields with assigned values are considered. Therefore if a license does not have a value for category and an advanced search criteria is defined as License Category != "Category 1", only those licenses with an assigned license category that is not equal to Category 1 will be returned.

# **FlexNet Code Insight Public APIs**

This section is a starting point for learning about the FlexNet Code Insight Public API. It will familiarize you with writing Groovy scripts for access to the FlexNet Code Insight Public APIs from several contexts.

- Public API Entry Points and Contexts
- Web UI Custom Buttons
- Detector Groovy Console
- Scan Server Autorun Scripts
- Workspace Reports
- Web Reports

## **Public API Entry Points and Contexts**

The following places in FlexNet Code Insight are accessible via the public APIs.

#### ScriptRunner

ScriptRunner is a standalone module that allows for communication with the FlexNet Code Insight Core and Scan servers to perform various application functions. For more information, see "Using ScriptRunner" in the *FlexNet Code Insight Installation and System Administration Guide*.

In addition, FlexNet Code Insight provides Groovy scripts that can be used to import and export group definitions and associated file information, such as tags applied to files, along with all attendant custom data. For information, see Importing & Exporting Workspaces in the *FlexNet Code Insight Installation and System Administration Guide*.

#### Web UI Administration Scripts Page

Custom Groovy scripts can be registered in the FlexNet Code Insight central database via a SQL script and can be executed via the Script option on the Administration page in the FlexNet Code Insight Web UI.

Note • These scripts are not interactive and therefore parameters cannot can be passed to the script.

#### **Web UI Custom Buttons**

Some FlexNet Code Insight customers have custom features and/or integrations that have been implemented using external Groovy scripts. These scripts are invoked by custom buttons in the FlexNet Code Insight Web UI that are activated by a FlexNet Code Insight license key (Code Insight.key) that enables such functionality. If your FlexNet Code Insight license key does not activate these features, the custom buttons will not be visible.

#### **Detector Groovy Console**

Groovy scripts may be executed from the FlexNet Code Insight Detector client either via the built-in Groovy console or via the Scripts menu. These scripts are limited to functionality available within a given FlexNet Code Insight workspace, and must operate within that context.

#### **Scan Server Autorun Scripts**

There are several FlexNet Code Insight scanner hooks that is used to execute custom logic at various phases of the workspace scan process. The following phases are supported: workspace open, on error, on success, before & after scan, after scan commit, and after post-scan analysis. These scripts are provided a WorkspaceCover object for convenience.

#### **Workspace Reports**

FlexNet Code Insight workspace reports in some cases have been implemented in Groovy and make use of FlexNet Code Insight public APIs. Workspace reports are provided a WorkspaceCover object and are limited to functionality available within a given FlexNet Code Insight workspace.

#### **Web Reports**

FlexNet Code Insight Web reports have all been implemented using Groovy scripts to allow customers to modify existing reports or create new ones.

## Accessing Core & Scan Servers via ScriptRunner

ScriptRunner is a standalone module that allows communication with FlexNet Code Insight Core and Scan servers to perform various application functions. For more information about ScriptRunner, see "Using ScriptRunner" in the *FlexNet Code Insight Installation and System Administration Guide*.



**Note** • If you are running ScriptRunner from a machine other than the FlexNet Code Insight Core Server, you must use the -c flag to specify the URL of the FlexNet Code Insight Core Server (i.e. http://Localhost:8888/Code Insight). If using ScriptRunner for the first time, you will be prompted for a password. Below are examples:

- On Windows: scriptRunner.bat -c <CORE\_SERVER\_URL> -u user file.groovy
- On Linux: ./scriptRunner.sh -c <CORE\_SERVER\_URL > -u user file.groovy

The following operations are supported via ScriptRunner. They are organized by various covers (facades) that expose the various APIs. For more information, see **API Covers (Facades)**.

Table 17-1 • Operation	n Types Supported	via ScriptRunner
------------------------	-------------------	------------------

Operation Type	Operation
Admin Service Cover	• User, Team, Project, and Policy Management
	<ul> <li>Metadata Value Management (User, Team, Policy, Task)</li> </ul>
	• Other Utility APIs
Metadata Service Cover	Metadata Field Management
Request Service Cover	Request Management
Reference Data Service Cover	Component, Version, License, and Vulnerability Management
	<ul> <li>Metadata Value Management (Component, Version, License, and Vulnerability)</li> </ul>
Project Data Cover	Project Configuration Management
	Workspace Management
	Project Queue (Scans + Reports) Management
	<ul> <li>Project Inventory Management (Comments, Questions/Answers, Checklist Items, and Review Status)</li> </ul>
	Project Request Management
	Project Task Management
	Project Snapshot Management
	• Metadata Value Management (Project, Workspace, Inventory, and Request)
Auditor Service Cover	Tag Management
	Group Management
	File Management
	• Metadata Value Management (File and Group)
Workspace Locator Cover	Open Existing Workspaces
Workspace Cover	Manage Workspace Settings
	Obtain Workspace Scan Results
	Codebase APIs

## **API Covers (Facades)**

FlexNet Code Insight public APIs are exposed via various covers (facades). These covers are the entry point for various service-level APIs that allow interfacing with the FlexNet Code Insight Core and Scan server.

- Admin Service Cover
- Metadata Service Cover
- Reference Data Service Cover
- Project Data Cover
- Auditor Service Cover
- Workspace Locator Cover
- Workspace Cover

## **Admin Service Cover**

The AdminServiceCover is the entry point for FlexNet Code Insight Core server administrative public APIs. It supports various operations related to managing users, teams, projects, and policies. To use these APIs, the AdminServiceCover needs to be instantiated by passing in the FlexNet Code Insight Core server IP address. An example is shown below.

#### Constructor

AdminServiceCover(String Code InsightCoreServerIpAddress)

#### **Sample Code**

import com.Code Insight.script.AdminServiceCover;

```
// Enter core server IP address
String coreServerIpAddress = System.getProperty("core.server.url");
AdminServiceCover adminSrv = new AdminServiceCover(coreServerIpAddress);
if (adminSrv != null) {
  try {
      // Print all team names
     adminSrv.getTeamNames().each {
        team ->
         println("Team: " + team);
      }
  } catch (Exception e) {
     e.printStackTrace();
   }
} else {
  println("Unable to connect to Code Insight Core server: " + coreServerIpAddress);
}
```

#### Metadata Service Cover

The MetadataServiceCover is the entry point for FlexNet Code Insight Core server metadata management public APIs. To use these APIs, the MetadataServiceCover needs to be instantiated by passing in the FlexNet Code Insight Core server IP address. An example is shown below.

#### Constructor

MetadataServiceCover(String Code InsightCoreServerIpAddress)

#### Sample Code

import com.Code Insight.script.MetadataServiceCover;

```
// Enter core server IP address
String coreServerIpAddress = System.getProperty("core.server.url");
MetadataServiceCover mdSrv = new MetadataServiceCover(coreServerIpAddress);
if (mdSrv != null) {
  try {
      // Print all metadata field/values for a particular license
      Object mdValue = null;
      long licenseId = 20; // Apache License, Version 2.0
        mdSrv.getMetadataDefinitions(mdSrv.getEntityId("license")).each {
            mdDef ->
            mdValue = mdSrv.getValue(mdDef.getId(), licenseId);
            // MDValue always returns a list even if single value, get first
            // value if list is not empty
            if (mdValue != null && mdValue.size() > 0) {
            println(" " + mdDef.getDisplayName() + ": " + mdValue.get(0));
        }
     }
   } catch (Exception e) {
      e.printStackTrace();
   }
} else {
  println("Unable to connect to Code Insight Core server: " + coreServerIpAddress);
}
```

#### **Reference Data Service Cover**

The ReferenceDataServiceCover is the entry point for FlexNet Code Insight Core server component, version, license, and vulnerability entity management public APIs. To use these APIs, the ReferenceDataServiceCover must be instantiated by passing the FlexNet Code Insight Core server IP address. An example is shown below.

#### Constructor

ReferenceDataServiceCover(String Code InsightCoreServerIpAddress)

#### **Sample Code**

import com.Code Insight.script.ReferenceDataServiceCover;

```
// Enter core server IP address
String coreServerIpAddress = System.getProperty("core.server.url");
```

```
ReferenceDataServiceCover refDataSrv = new ReferenceDataServiceCover(coreServerIpAddress);
if (refDataSrv != null) {
    try {
        // Print all license family names
        refDataSrv.getLicenseFamilies().each {
            licId ->
            println("License Family: " + refDataSrv.getLicense(licId).getName());
        }
    } catch (Exception e) {
        e.printStackTrace();
    }
} else {
    println("Unable to connect to Code Insight Core server: " + coreServerIpAddress);
}
```

## **Project Data Cover**

The ProjectDataCover is the entry point for FlexNet Code Insight Core server project data management public APIs. To use these APIs, the ProjectDataCover must be instantiated by passing the FlexNet Code Insight Core server IP address. An example is shown below.

#### Constructor

ProjectDataCover(String Code InsightCoreServerIpAddress)

#### Sample Code

import com.Code Insight.script.ProjectDataCover;

```
// Enter core server IP address
String coreServerIpAddress = System.getProperty("core.server.url");
ProjectDataCover pdCover = new ProjectDataCover(coreServerIpAddress);
if (pdCover != null) {
  try {
      // Print all inventory items for project
      String teamName = "Engineering";
      String projectName = "ePortal 1.3";
      pdCover.getInventoryForProject(teamName, projectName).each {
         invItem ->
         println("Inventory Item: " + invItem.getAuditGroupLabel());
     }
  } catch (Exception e) {
     e.printStackTrace();
   }
} else {
  println("Unable to connect to Code Insight Core server: " + coreServerIpAddress);
}
```

## **Auditor Service Cover**

The AuditorServiceCover is the entry point for auditor APIs related to groups and tags. To use these APIs, the AuditorServiceCover must be instantiated by passing the FlexNet Code Insight Core server IP address. An example is shown below.

#### Constructor

AuditorServiceCover(String Code InsightCoreServerIpAddress)

#### Sample Code

import com.Code Insight.script.AuditorServiceCover;

```
// Enter core server IP address
String coreServerIpAddress = System.getProperty("core.server.url");
AuditorServiceCover auditCover = new AuditorServiceCover(coreServerIpAddress);
if (auditCover != null) {
  try {
     // Print all groups for project
     int projectId = 1;
      auditCover.getGroupIds(projectId).each {
        groupId ->
        println("Group: " + auditCover.getGroupDetails(groupId).getName());
     }
  } catch (Exception e) {
     e.printStackTrace();
  }
} else {
  println("Unable to connect to Code Insight Core server: " + coreServerIpAddress);
}
```

### Workspace Locator Cover

The WorkspaceLocatorCover is instantiated by ScriptRunner and provided as a variable called locator. The locator is used to open a workspace. An example is shown below.

#### Constructor

import com.Code Insight.script.WorkspaceCover;

#### **Sample Code**

```
// Enter scan server IP address
String scanServerIPAddress = "127.0.0.1";
String workspaceName = "ePortal_13";
String serverUri = "http://" + scanServerIPAddress + "/";
String workspaceUri = serverUri + workspaceName;
locator.setServerUri(serverUri)
WorkspaceCover workspace;
try {
  workspace = locator.openWorkspace(workspaceUri);
  println("Workspace Name: " + workspace.getName());
  println("Workspace UUID: " + workspace.getUuid());
} catch (Exception e) {
  e.printStackTrace();
} finally {
   if (workspace) {
      workspace.close(); // Make sure you always close a workspace you open
   }
}
```

### **Workspace Cover**

The WorkspaceCover is the entry point for workspace scan results and codebase access APIs. To use these APIs, the WorkspaceLocatorCover must be used to obtain a WorkspaceCover object that represents an open workspace. The WorkspaceCover can then be used to obtain access to the following covers that contain APIs for workspace scan results and codebase access:

#### CodebaseServiceCover

This is a deprecated cover and should not be used. Use the WorkspaceCover.getFilesystem() API instead to gain access to the codebase (files in the file system) that was scanned by the workspace.

#### ScanResultCover

This cover is used to obtain high-level information about the latest scan including the Compliance Library version, the scan date and duration, and the various file counts associated with the workspaceultServiceCover.

This cover is used to obtain scan results for a given workspace. There are APIs provided to obtain any scan results that can be viewed by the auditor in the Detector client.

#### SignatureServiceCover

This cover is used to obtain information about files, Java names, and releases known to a given workspace.

#### **Sample Code**

Below is an example for showing the number of scanned files and detected copyright holders:

```
import com.Code Insight.script.WorkspaceCover;
```

```
// Enter scan server IP address
String scanServerIPAddress = "127.0.0.1";
String workspaceName = "ePortal_13";
String serverUri = "http://" + scanServerIPAddress + "/";
String workspaceUri = serverUri + workspaceName;
locator.setServerUri(serverUri)
WorkspaceCover workspace;
try {
  workspace = locator.openWorkspace(workspaceUri);
  println("Workspace Name: " + workspace.getName());
  println("Workspace UUID: " + workspace.getUuid());
  println("Scanned Files: " + workspace.getScanResult().getScannedFileCount());
  println("Detected Copyright Holders...");
  workspace.getScanResultService().getCopyrightOwners().each {
     holder ->
      println(" " + holder.getName());
  }
} catch (Exception e) {
  e.printStackTrace();
} finally {
  if (workspace) {
      workspace.close(); // Make sure you always close a workspace you open
   }
}
```

1	8

# **Auditing and Analysis Overview**

This section provides an overview of the what, how, and why auditors perform the tasks associated with their role.

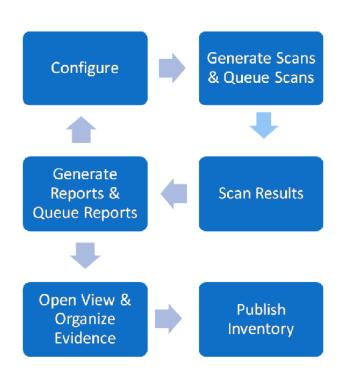
- Tasks an Auditor Performs
- How Auditors Perform Tasks
- Why Auditors Perform Tasks

### **Tasks an Auditor Performs**

An auditor has the job of analyzing evidence but not performing Intellectual Property (IP) compliance and vulnerability problem-solving actions. The general auditing and analysis steps are as follows:

- 1. Setting up the workspaces to scan codebases for third-party materials
- 2. Scheduling scans and reports
- 3. Launching Detector
- 4. Viewing scan and reports in the task queue
- 5. Viewing reports
- 6. Choosing the workspaces to open and analyze
- 7. Opening and accessing scan results
- **8.** Viewing different types of evidence (for example, source code fingerprint matches, exact files [digest] matches, copyright matches, license matches, string search term matches, Java name matches, etc.)
- 9. Organizing and viewing the codebase scan evidence
- 10. Analyzing the codebase scan evidence and constructing groups and components to represent detected inventory
- **11.** Publishing groups as inventory
- 12. Managing a catalog of custom Open Source Software (OSS) material

A general view of the auditor workflow is presented in the following diagram. If the scan is not providing you with the information you are seeking, you can re-configure the workspace and schedule a new scan to analyze.



### Workspace / Project

### **How Auditors Perform Tasks**

An overview of the way an auditor performs the various tasks is as follows:

- 1. Configure the workspace settings and details. This includes file settings, detection techniques to employ during the scan, sensitivities of the results, and specifics about the types of files to scan, such as extensions, etc.
- 2. After the workspace is configured, schedule scans and reports of the codebase in one or many workspaces.
  - **a.** Scanning is best done in batches. To save time, queue your scans before leaving work. This way they can be sequentially performed through the night and not during work hours. Depending on the size of your code base, some scans and/or reports may take many hours.
  - **b.** Forensic scans allow you to generate reports that categorize underlying evidence. The advantage of this is that you can look at reports, for example, while on an airplane without network connectivity, by printing out a static hard copy.
  - **c.** Scan results are live on the server, and unless you change a code base or data library you don't need to scan a workspace again. Reports are persistent on the scan server.
- 3. Check the specific task queues to make sure you have scheduled and prioritized the scans and reports to your liking.

- **4.** Once the scans are completed, launch Detector from the Web UI. The Detector forensic client allows you to choose one workspace from your completed list of scans and view, with varying levels of granularity, every piece of data (scan results) in that specific workspace's code base.
- 5. Analyze any evidence that might constitute a relevant compliance or security vulnerability issue in your code base. The evidence you analyze includes source code fingerprint matches, exact files [digest] matches, detected copyrights, detected license text or references, string search term matches, detected emails and URLs, Java name matches, etc. Sometimes there is an issue, but it has low relevance to your eventual software application's integrity. For example: You find an issue with a certain license match. But this license match issue is only relevant if you are distributing your codebase internationally. If your company has no history or intention of distributing your application internationally, you do not have a licensing issue that requires attention.
- **6.** Organize and evaluate the information as it relates to your own internal compliance and security vulnerability policies.
- 7. Publish an inventory of components that are detected via the scan of the code base. These inventory items are then put through the compliance workflow to ensure that usage is permissible in your organization. This workflow may involve the security analysts, owner, and various reviewers.
- **8.** Inventory with associated component versions containing known security vulnerabilities will require a review by the security analyst. Furthermore, all inventory items require an IP review by the reviewers, and these are configured by the project review workflow.

### **Why Auditors Perform Tasks**

The main job function of the auditor is to analyze the results of the codebase scan, and generate an inventory (bill of materials) using the automated detection techniques as well as the other available third- party indicator evidence that resulted from the scan. By subsequently publishing the detected inventory, issues related to IP compliance and security vulnerabilities can be brought to the attention of the rest of the team.

The auditor does not make any compliance decisions. His or her sole responsibility is to analyze the scan results and generate a complete and accurate inventory of third-party materials. Once the inventory is published the rest of the workflow determines the validity of the existence of the inventory items.

#### Chapter 18 Auditing and Analysis Overview

Why Auditors Perform Tasks

1	9

# **Configuring Workspaces**

This section contains the following topics:

- Workspaces
- Accessing Workspace Configuration Settings
- General Tab Tasks
- Software Configuration Management Tab
- Detection Tab Tasks
- Source Code Options Tab
- Rescan Options Tab
- Automated Analysis Tab

### Workspaces

The owner or assigned auditor configures project workspaces before launching a project. Workspaces are associated with specific projects and are usually scanned to ensure code compliance and to discover security vulnerabilities associated with the detected components.



**Note** • Only letters, numbers, underscores, and dashes may be used in the workspace name. To access workspace configuration settings, perform the following steps.

# Accessing Workspace Configuration Settings

To access workspace configuration settings, perform the following steps.



#### To access workspace configuration setting, do the followings:

**1.** Log in to FlexNet Code Insight as the *Auditor*.



2. You can get to the list of your active projects from the **Dashboard** or by clicking **My Projects** in the main menu.

G Home		6			Q
New request	O requests submitted by me	0 reques	ts assigned	to me	Search requests
Filter: My Active Projects	My Tasks Ay Shortcuts Dashboard	٩			
Project 🔺	Audit (does not include files within archives)	Inventory Review		Inventory with Legal / Rem	ediation / Security Issues
ePortal-1.3	0 of 44 files with indicators reviewed	There are no inventory item	s for this project.	There are no inventory iter	ms for this project.
4 4   Page 1 of 1	0 of 34 files without indicators reviewed   ▶ ▶    ⊉   Show All				1 - 1 of

#### Figure 19-1: My Projects Dashboard

Basic Search Advanced Search   Filter: In Progress	Projects Y Search:			P			
Name 🔺	Team	Owner	Status	Inventory	Requests	Tasks	Actions
ePortal Project	Team1	Auditor Auditor	In Progress	0	0	2	0 7 0



3. Click the project name (Name column) or the Magnifying Glass icon (Actions column). The Summary tab appears.

ePortal 1.3 (Enterprise )	portal application, version 1.3.)					
Summary Workspaces	nventory Requests Tasks Policies Comments					
Name	ePortal 1.3 (Enterprise portal application, version 1.3.)					
Team	Engineering (San Jose development team.)					
Owner	Owner Smith					
Auditors	Auditor Smith					
Security Analysts	There have been no Security Analysts selected for this project.					
Observers	There have been no Observers selected for this project.					
Advanced Options	Enable Inventory Quick Review: Yes       Project Summary Emails: Never         Auto-Publish Inventory: Yes       Request Review Reminder Emails: Never         Apply Policies to Inventory: Yes       Request Form: Short Request Form Definition					
Comments	There are no comments for this project					
Child Projects	There are no child projects for this project.					
Status	In Progress					
Progress	Audit  12 of 43 files with indicators reviewed  6 of 35 files without indicators reviewed  Inventory Review  7 total (1 rejected, 1 pending review, 4 approved, and 1 not yet reviewed)  Inventory with Legal / Remediation / Security Issues					
	Legal: 7 total (0 open, 0 completed, and 7 none required)					
	Remediation: 7 total (1 open, 0 completed, and 6 none required) Security: 7 total (0 open, 0 completed, and 7 none required)					

- **4.** Select the **Workspaces** tab, which shows the project compliance and vulnerability workspaces associated with the project. The icons to the right of the project name allow you to perform the following activities:
  - View and edit workspace details (magnifying glass).
  - View and edit workspace settings (cog).
  - View the task queue for the selected workspace (clock).
  - View reports for the selected workspace (graph).
  - Launch the Detector forensic client for the selected workspace (computer monitor).

ePortal 1.3 (Enterprise p	ortal application, version 1.3.	)	
Summary Workspaces	Inventory Requests Ta	sks Policies Comments	
Search:		R	Create New Workspace
Name 🔺	Server	Audit Progress	Actions
ePortal_13	server1	12 of 43 files with indicators reviewed 6 of 35 files without indicators reviewed	Q 🔅 🛇 🌌 県

### **General Tab Tasks**

To configure Workspace Settings on the General tab, perform the following steps.



#### To set workspace settings on the General tab, do the following:

#### 1. Click My Projects > Project Name > Workspaces Tab >Cog icon. The General tab appears:

ePortal	1.3 → Workspa	$ce \rightarrow ePortal_{1-3}$	Settings				
General	Detection Sc	ource Code Options	Rescan Options	Automated Analysis			
Name		ePortal_1-3					
Descripti	ion						
Applicat	long						
		None (Use Loo	al File System)				
Folders t	to Scan	C:\Cleanroon	n\ePortal-1.3\		Browse		
					Туре		
					Remove		
Exclude	d File Patterns	*শ্*_jsp.java *গ্.hg *গ্.svn *গ্CVS		· · ·			

2. The General tab allows you to enter a description for the workspace. If you are scanning a snapshot of your code base that is not tied to an SCM system, you can also choose folders to scan by clicking the Browse, Type, or Remove buttons. Note that the folders to scan may be restricted by the group to which this project belongs. The Application Administrator can restrict which folders are available for groups to scan by assigning the folder group permissions. Clicking on the Type button opens a dialog box requesting that you input a scan folder. To add a file pattern to exclude during a scan, click the Plus icon. The Minus icon removes excluded file patterns, so these files now appear in a scan.



Note • Windows hard links are not respected by the scanner and may cause file counts to be off in the workspace.

3. Click Save.

### **Software Configuration Management Tab**

If integration with ClearCase, Perforce, Subversion, Git, or TFS is enabled in the scan engine SCM configuration file (<CODE\_INSIGHT\_ROOT>/config/scanEngine/scm.properties), the **Applications** pull-down menu in the Workspace Settings – General tab is populated with the available options.

Selecting any of the options enables the **Software Configuration Management** (SCM) tab which allows you to configure the SCM settings for the selected SCM application for the current workspace. Doing this ensures that files are up to date at the time of scanning.

See the *Installation and System Administration Guide* for detailed instructions related to SCM configuration for workspaces and project copy.

### **Detection Tab Tasks**

Task	То	configure workspace settings on the Detection tab, do the following:
	1.	To access the Detection tab screen, follow the instructions in the General Tab Tasks.
	2.	Click the Detection tab. The Detection tab screen allows you to set the detection parameters. For example, you can enable digest matching, namespace matching, copyright file patterns, language extensions, source code fingerprint scanning, and string searches.
	3.	You can choose to exclude or include in the scan specific code languages and file extensions associated with those languages. To see the file extensions associated with the language that will be included in the scan, highlight a language and then select the <b>Enable</b> checkbox.

To configure Workspace Settings on the Detection tab, perform the following steps.

ociated with those an, highlight a iguag

- 4. Configuring Archives Scanning—Check the Scan Files Inside Archives checkbox to perform a deep scan on the archives in your codebase. With this option enabled, the archive's outer file (such as foo.jar) and its inner files (all files inside foo.jar) are tagged for different evidence types. Both types of files will be visible in Detector, allowing you to perform file operations such as marking, tagging and adding to group.
- 5. The following table lists the supported archive types and evidence.

Table 19-1 • Supported Archive Types and Evidence

Supported Types	Description
Supported Archive Types	ab, ear, jar, rpm, sar, tar, tar.bz, tar.bz2, tar.bzip2, tbz, tgz, war and zip are supported archive types. For the most up-to-date information on supported types, go to Workspace Settings -> Detection Tab -> Archive Scanning Options section at the bottom of the page to see a list of extensions supported in this release.
Supported Evidence Types	Exact Matches, Copyrights, Emails and URLs, Search Terms and Licenses are supported evidence types. Automated Analysis techniques such as Auto- WriteUp, POM File Analyzer and MID Rule Detection are also available for archives. See the Automated Analysis Tab section on how to enable these techniques.
Source Matches	Files inside archives will not be scanned and tagged for Source matches. For extended analysis on files inside archives, it is recommended that you manually unpack the archive before performing a scan.
Exact Matches	Archives that contain an Exact match (digest match) on the outer file will be tagged with the "Contains Exact File Matches" tag. Inner files of these archives will not be tagged for Exact matches. This behavior is in place as a performance enhancement and is reflected in the group/tag file counts. Inner files of archives with Exact matches will still be tagged for all other evidence types, including Copyrights, Emails and URLs, Search Terms and Licenses.

6. You can specify which archive types to include for deep scanning in the Archive Scanning Options section. To specify an archive type for deep scanning, select the extension associated with the archive from the list of available extensions. Use the < option to move the item to the Scan Files Inside These Archives area on the left. If you do not want to include an archive type for deep scanning, use the > option to move the extension to the Don't Scan Files Inside these Archives area on the right. For information on viewing and analyzing scan results for archive files, see Working with Archives.

General Detection Source Code Options	Rescan Options Automated Analysis
Enable Digest Matching	8
Enable License Detection	
Enable Email / URL Detection	8
Enable Namespace Matching	8
Copyright File Patterns Enable ♂	
Languages - Extensions Enable Source Code Fingerprint Scannin	g
Don't Fingerprint Files with Digest Match	es 🗹 * If checked, files that have digest matches will not be source code fingerprinted. Scans will take longer if this option is disabled.
String Search	* Short search strings may negatively impact scan time.
Archive Scanning Options	Scan Files Inside Archives  I unchecked, files within the archive will not be scanned or visible.  Scan Files Inside These Archives  Cab ear jar rpm

7. To search the code base for a certain string, click the Plus icon in the **String Search** row. The Input dialog appears so you can enter the exact text string for which to search.

Input			×
2	Please input the n	ew search string:	
		Const	
	OK	Cancel	

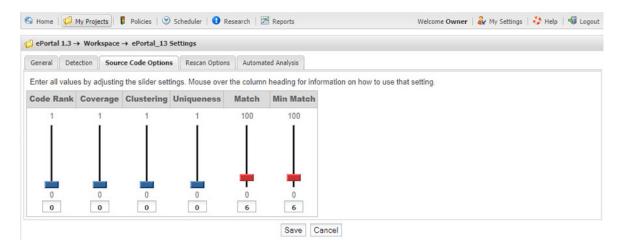
8. Click OK to save your detection settings.

# **Source Code Options Tab**

To set the sensitivity of the workspace scan of the source code scan, perform the following steps.

#### To set the sensitivity of the workspace scan of the source code scan, do the following:

- 1. To access the **Source Code Options** tab, follow the instructions in the General Tab Tasks section.
- 2. Select the **Source Code Options** tab. The **Source Code Options** tab opens. You can adjust the sliders to narrow the percentages of certain code elements and characteristics you want to see in a scan. This allows you to save time by analyzing priority compliance issues instead of every issue that might appear in a code base.



3. The sliders act as scan thresholds. All source matches with values below the sliders will be suppressed from the scan results. For example, if you set the Coverage slider to .75 (75 percent coverage), then the scan results will only source matches with a coverage value above 75%. All other matches will not be available. *Coverage* is a term used to identify the percentage of third-party files detected in the scanned source file.

### **Rescan Options Tab**

The options on this tab allow you to control the conditions under which files that have been reviewed by the auditor are brought out of review during a rescan.



Ŷ

Task

To configure workspace settings on the Rescan Options tab, do the following:

- 1. To access the Rescan Options tab, follow the instructions in General Tab Tasks.
- 2. Select the **Rescan Options** tab to view available options.

General Detection Source Cod	le Options Rescan Options Automated Analysis			
Enable Incremental Scanning	N			
File Review Status Options	<ul> <li>Below are several options to control which changes to scan results will bring a file back to Unreviewed state following a rescan. Only files that have been marked as Reviewed and NOT marked as Analysis Completed will be changed.</li> <li>Digest (Exact) Matches Flip to unreviewed state if a file had digest matches in the previous scan, but no longer does, or did not have any digest matches in the previous scan, but now longer does, or did not have any digest matches in the previous scan, but now does.</li> <li>Copyrights Flip to unreviewed state if the list of detected copyright holders in a file is different following a rescan.</li> <li>Licenses Flip to unreviewed state if the list of detected licenses in a file is different following a rescan.</li> <li>Emails and URLs Flip to unreviewed state if the list of detected email addresses or URLs in a file is different following a rescan.</li> <li>Search Terms</li> </ul>			
	<ul> <li>Flip to unreviewed state if the list of detected search terms in a file is different following a rescan.</li> <li>Source Matches</li> <li>Flip to unreviewed state if the source match results in a file are different following a rescan.</li> <li>Flip to unreviewed state if the only change in scan results for that file is that there are fewer components in the list of possible source matches after a rescan.</li> <li>Ignore Unchanged Files</li> <li>Do NOT flip to unreviewed state if the file has not changed since the last scan.</li> </ul>			

You may disable incremental scanning and force a complete re-scan of the selected codebase. Incremental scans only scan files that have been added or modified since the last scan. The entire codebase is scanned during the first scan, or it is scanned if the Compliance Library is updated.

- **3.** Select any of the following options to control which changes in the scan results will return a file to an unreviewed state after a rescan:
  - **Digest (Exact) Matches**—Return to unreviewed state if a file had digest matches in the previous scan, but no longer does, or did not have any digest matches in the previous scan, but now does.
  - **Copyrights**—Return to unreviewed state if the list of detected copyright holders in a file is different following a rescan.
  - Licenses—Return to unreviewed state if the list of detected licenses in a file is different following a rescan.
  - **Emails and URLs**—Return to unreviewed state if the list of detected email addresses or URLs in a file is different following a rescan.
  - **Search Terms**—Return to unreviewed state if the list of detected search terms in a file is different following a rescan.
  - Source Matches—Return to unreviewed state if the source match results in a file are different following a rescan.
    - Return to unreviewed state if the only change in scan results for that file is that there are fewer components in the list of possible source matches after a rescan.
  - Ignore Unchanged Files—Do not return to unreviewed state if the file has not changed since the last scan.

Note • Only files that have been marked as Reviewed and not marked as Analysis Completed will be changed.

### **Automated Analysis Tab**

To control which automated analysis techniques are executed after the scan completes, perform the following steps. (Refer to Automated Analysis for more details about these techniques.)

Task

To configure workspace settings on the Automated Analysis tab, do the following:

- To navigate to the Automated Analysis tab, select My Projects > project\_name > Workspaces>workspace\_name>Workspace Resources>Edit Workspace Settings.
- 2. Open the Automated Analysis tab:

General	Detection	Source Code Options	Rescan Options	Automated Analysis			
							Automated Analysis Guide
Enable I	POM File An	alyzer					
Enable /	Auto-WriteU	p™					
Enable I	Multi-Indicat	or Detector	<b>«</b>				
Add Nor	n-Indicator F	iles to Groups?					
Enable /	Analyzer						
Enable (	CodeAware						
		space was previous ent scans, as this ca			recommended not to enable C	odeAware (either in con	junction with or in place of
				Save	Cancel		

- 3. Select any of the following options for the automated analysis of the scan results for a workspace:
  - Enable POM File Analyzer—This automatically creates a group for the artifact for which the POM file exists, as well as for each dependency that is defined in the POM file. The dependency groups also contain the group id of the parent group in the newparentIds field. This data can be used to generate a hierarchical relationship between the top-level projects and their transitive dependencies. This analysis technique is disabled by default.
  - Enable Auto-WriteUp<sup>™</sup>—This automatically creates a group with associated files and populates it with group details such as Description, URL and As-Found License Text if all rule engine conditions are satisfied. For detailed information on this option, see Using Auto-WriteUp<sup>™</sup>. This analysis technique is enabled by default.
  - Enable Multi-Indicator Detector (MID)—This automatically creates a group with associated files if all MID rule conditions are satisfied. This analysis technique is enabled by default.
  - Add Non-Indicator Files to Groups—For each system group that is created, the indicator files (files that are
    indicators of the group and the reason the group exists) are always added to the group. However, you can also
    optionally have the system add all otherfiles known to exist in the component (and version if available)
    associated with the group. In other words, any scanned file that has exact matches to the component (and
    version if available) can be added as an included file to the system created group. This option is disabled by
    default.
  - Enable Analyzer—The Analyzer aids the auditing of third-party code by automatically identifying dependencies, packages, and source distributions. The Analyzer works in two ways. First, it can be used before a scan task to generate a Quick Assessment report that provides an overview of your codebase contents. Secondly, the Analyzer can execute automatically (or be scheduled to execute) after a scan to create component groups or inventory items. It also builds Third-Party Notices for groups and inventory items when the data is available and, for scheduled executions, produces a Group Builder report. Refer to Using the Analyzer to for details.

• Enable CodeAware—CodeAware is basically the "next generation" of automated discovery, providing much of the same detection functionality as the Analyzer to build groups and auto-generate inventory. If you run CodeAware, the recommendation is *not* to enable any other analysis technique on the **Automated Analysis** tab. This recommendation is in place to avoid duplicate groups either on the initial scan or in subsequent scans.



**Note** • If a workspace was previously scanned with the Analyzer, you are strongly recommended not to enable CodeAware in place of the Analyzer for subsequent scans, as this can result in duplicate groups. If you would like to replace Analyzer results with CodeAware results, you can do so in a new project to avoid duplicates.



# **Automated Analysis**

After a scan, the system runs a set of automated analysis techniques to sort through the scan results and create system groups with associated files, each group representing an automatically-detected inventory item. The system groups can then be promoted to inventory by way of auto-publishing or manually publishing. The following techniques are available:

- POM File Analyzer
- Auto-WriteUp<sup>™</sup>
- Multi-Indicator Detector (MID)
- Analyzer
- CodeAware

For a comparison of features supported by these techniques, see the later section, Comparison of the Analysis Techniques.

Refer to Automated Analysis Tab for instructions on how to enable one or more of these analysis techniques for scans on project workspaces.

### **POM File Analyzer**

This analysis technique performs dependency checking of Maven's Project Object Model (POM) files. POM files are XML representations of the structure of a Maven project and are contained in a pom.xml file. If you enable this option, the scanner automatically creates a group for the artifact for which the POM file exists, as well as for each dependency defined in the POM file. The dependency groups also contain the group id of the parent group in the new **parentIds** field. This data can be used to generate a hierarchical relationship between the top-level projects and their transitive dependencies.



Note • This analysis technique is disabled by default.



To view parent groups that the current group is a dependency of in the POM file, do the following:

1. Click the Parents hyperlink in the Group Id field. The Parent Groups dialog appears:

🛓 Parent	t Groups	×
ID 🔬	Name	
21	POM - acegi-security (1.0.7)	

This dialog displays all parent groups that declare the current group as a dependency in the POM file. If enabled, POM File Analyzer will be applied to files inside archives.

2. When you finish viewing the dependencies, click the X to close the dialog.

### Auto-WriteUp™

This analysis technique is based on a rule engine that automatically identifies OSS content in the codebase. It creates groups that are populated with group details such as Description, URL and As-Found License Text. If enabled, Auto-WriteUp is applied to files inside archives. In the majority of cases, the Auto-WriteUp data is curated by the data library team and verified for accuracy.

For more information, see Using Auto-WriteUp™.



**Note** • Auto-WriteUp is enabled by default.

## Multi-Indicator Detector (MID)

This analysis technique relies on rules such as MD5-matching and filepath-matching to automatically identify OSS content in the codebase. It creates groups with associated files if all the MID rule conditions are satisfied. This analysis technique is enabled by default.

MID rules are shipped with FlexNet Code Insight and are added to the central database as part of the installation process. User-specified MID rules are unique to each FlexNet Code Insight Scan Server, and it is up to the user to keep them synchronized across all servers in case of a multi-scan server installation. The user-specified MID rules are defined in a Microsoft<sup>®</sup> Excel<sup>®</sup> spreadsheet that the system reads each time a workspace is scanned. It is not necessary to bounce the FlexNet Code Insight Scan Server if a change is made to the MID rules spreadsheet. The MID rules spreadsheet can be found at the following location on the FlexNet Code Insight Scan Server:

<CODE\_INSIGHT\_ROOT\_DIR>\6.13.x\config\scanEngine\multi\_indicator\_detector.xls

Each row in the MID rule spreadsheet represents a single MID rule.

The following columns are used to notify the FlexNet Code Insight Scan engine which component and version (if known) is to be selected for the system group:

- **Rule Notes**—The value entered into this column shows up as the detection evidence value for a system-generated group. It is the explanation as to why a particular group was created. This value is optional.
- **Component ID**—The ID of the component to be associated with the system-generated group. You can look up a component id using the Research page of the FlexNet Code Insight 6.13.*x* web application. The component ID must exist in the system for the rule to be evaluated; otherwise the rule is skipped. This value is required.
- **Version ID**—The ID of the component version to be associated with the system-generated group. You can look up a component version ID using the Research page of the FlexNet Code Insight 6.13.x web application. The component version ID must exist in the system for the rule to be evaluated; otherwise the rule is skipped. This value is optional.

The following data may be used as criteria for MID rule conditions; at least one condition is required for each MID rule:

- File Path Pattern—File name or path to be considered for MID rule analysis; if path criteria are not met, the rule is skipped with no further processing (for example:\*.dll).
- **MD5 Digest**—The MD5 digest of the file may be used as the most basic criteria, if the file has the following MD5 digest, then it is component Foo, version #.#. If the MD5 criteria are used, the search term and namespace conditions are not evaluated.
- Search Terms—All of the specified search terms must exist in the file for this condition to evaluate to true.
- Java Names—All of the specified Java names must exist in the file for this condition to evaluate to true. If a single package name is specified, the rule will match a java source file or class file that belongs to the specified package or package with the specified prefix (for example, com.foo will match any package that starts with com.foo). It will also match an archive file (.jar,.war,.ear,.zip)which contains a file that matches the package name. If multiple names are given, the rule will only match an archive file that contains all the specified packages.

### Analyzer

The Analyzer technique uses a variety of methods to identify OSS content such as packages, source distributions, and dependencies. It creates groups and, optionally, a Group Builder or Quick Assessment workspace report. Analyzer detection methods include various package, search term, repository, digest and component analyzers with optional data lookups via Data Services (see Data Services). You can find details about the files and methods of detection used by the Analyzer in the **Detection Notes** group field. There are three ways to invoke analyzer:

- Analyzer as Part of Scan—As of version 6.13.1, the Analyzer automatically executes at the end of scans as long as it is enabled on the **Automated Analysis** tab for a project workspace (this is the default setting). If invoked in this manner, Analyzer creates groups for identified OSS content but does not generate a report.
- **Group Builder**—You can use the **Schedule Scan/Report** feature to schedule a scan that is followed by the generation of the Group Builder report. This method creates groups for identified OSS content (the same set of groups as created by invoking Analyzer as part of scan) and generates the Palamida Analyzer Group Builder report. This workspace report also includes a Bill of Materials, Security Vulnerability information, Third-Party Notices information and Codebase Metrics for the given workspace. Note that the report requires at least one successful scan prior to execution of the report.
- Quick Assessment—Alternatively, you can use the Schedule Scan/Report feature to schedule the Quick Assessment report. This workspace report does not require a scan prior to execution of the report. It provides a quick overview of the codebase contents and includes a Bill of Materials, Security Vulnerability information, Third-Party Notices information and Codebase Metrics.

#### **Data Services**

The Analyzer uses Flexera's Data Services (DS) to supplement license information, component metadata, and known security vulnerabilities for the detected groups. Data Services (DS) is a RESTful API hosted on Amazon Web Services. DS provides information about Open Source projects from the FlexNet Code Insight Data Library. Requests to Data Services take the form of an "HTTPS GET" request to the web service.

Files and code snippets are never sent to Data Services. The web service is only queried for information about Open Source projects as contained in the FlexNet Code Insight Data Library (for example, component information, vulnerabilities, licenses, digest-to-component data and so on) to enable rich inventory building.

#### **Analyzer Requirements**

The Analyzer requires outgoing TCP access on port 443 to access Data Services. Proxy support can be enabled in analyzer.properties. Depending on the security policy of your organization, the following URL may need to be added to the security policy white list: https://api.palamida.io.

### **CodeAware**

CodeAware is basically the "next generation" of automated discovery, providing much of the same analysis functionality as the Analyzer to build groups and auto-generate inventory with relevant details, license and vulnerability information. CodeAware detection methods include package, search term, repository, digest, and component analyzers, as well as other intelligent parsing algorithms and live lookups. CodeAware detects various packages and source distributions. You can find details about the files and methods of detection used by CodeAware in the **Detection Notes** group field.

The CodeAware analysis technique is first introduced in 6.13.1 with limited functionality. While it performs accurate detection and builds groups/inventory, other CodeAware capabilities (for example, population of As-Found License Text, determination of group Priority, live vulnerability lookups, detection inside archives, and the processing of dependencies) will be available in subsequent releases only. Refer to Comparison of the Analysis Techniques for more information on the existing capability of CodeAware and the other automation techniques.

If you run CodeAware, the recommendation is *not* to enable any other analysis technique available on the Automated Analysis Tab. This recommendation is in place to avoid duplicate groups either on the initial scan or in subsequent scans.

**Note** • If a workspace was previously scanned with the Analyzer, you are strongly recommended not to enable CodeAware in place of the Analyzer for subsequent scans, as this can result in duplicate groups. If you would like to replace Analyzer results with CodeAware results, you can do so in a new project to avoid duplicates.

#### **CodeAware Requirements**

CodeAware requires outgoing TCP access on port 443 to access known repository sites for license, vulnerability and other information. CodeAware performs only lookups and never sends files or code snippets. Depending on the security policy of your organization, the following URLs may need to be added to the security policy white list:

- https://spdx.org/licenses/
- https://search.maven.org/
- https://rubygems.org/api/v1/gems/
- https://registry.npmjs.org

- https://registry.bower.io/packages/
- https://packagist.org
- https://api.nuget.org/v3-flatcontainer/
- https://oss.sonatype.org
- https://api.bintray.com

#### For vulnerability:

- https://nvd.nist.gov
- https://web.nvd.nist.gov/view/vuln/detail

#### Other:

https://www.flexerasoftware.com\*\*

### **Comparison of the Analysis Techniques**

All the analysis techniques described in this chapter generate *groups*, which are groupings of files identified by the same third-party component, version, and license (although a license might not be available for some dual or multi-licensed groups). Groups can then be automatically or manually *published*—that is, promoted to inventory and made available in Code Insight's Web user interface for further review and inclusion in your product's Bill of Materials.

The following table provides a comparison of other important features (aside from group creation) that these various analysis techniques support:

	Detects dependencies (direct)	Detects dependencies (transitive)	Processes files inside archives	Populates additional group details	Populates As-Found license text	Supports custom rules	Creates custom versions
POM Analyzer	pom.xml only	No	Yes	No	No	No	No
MID Rules	No	No	Yes	No	No	Yes	No
Auto-WriteUp	No	No	Yes	Yes	Yes	Yes	No
Analyzer	Yes	pom.xml only	Yes	Yes	Yes	No	Yes
CodeAware	No *	No *	No *	Yes	No *	No *	Yes

#### Table 20-1 • Comparison of Analysis Techniques

\* Available in a future release.

**Chapter 20** Automated Analysis Comparison of the Analysis Techniques

Company Confidential FNCI-6131-UG00 FlexNet Code Insight 6.13.1 User Guide



# Using Auto-WriteUp<sup>™</sup>

This section discusses the Auto-WriteUp<sup>™</sup> feature in the following topics:

- Auto-WriteUp<sup>™</sup>
- Configuring Auto-WriteUp™
- Frequently Asked Questions

### Auto-WriteUp™

Auto-WriteUp<sup>™</sup> is part of the automated analysis technologies distributed with FlexNet Code Insight to assist the user with the auditing process. Based on a rules engine, Auto-WriteUp<sup>™</sup> can automatically identify OSS content in a scanned code base and create populated groups in the FlexNet Code Insight Detector Client. Auto-WriteUp<sup>™</sup> is part of the automated analysis technologies distributed with FlexNet Code Insight to assist the user with the auditing process.

rkspace Script About							
	la surla ra la						
elcome Groups Tags Filters Components Licenses	Emails/Uris Search Terms Cop						
Name         Priority         Co.           05         Apache Axis 1.4 (Apache 2.0)         3 - Med apa           1         Apache BCEL 5.1 [bundled with Ed	che-axis Apache License che-boel Apache License che-boel Apache License che-camel Apache License che-camel Apache License	e 1.1 Auto-WriteUp (Palamida) Yes 06/ No In Un U Unknown 1 1 e 1.1 Auto-WriteUp (Palamida) Yes 06/ No In Un U Unknown 1 1					
08 Apache Cassandra 1.0.0 (Apache 3 - Medi apa 05 Apache Commons BeanUtils 1.8.3 3 - Medi apa	die	A REAL PROPERTY OF REAL PLANE AND A REAL PROPERTY OF REAL					
30         Apache Commons HttpClient 3.1 ( 3 - Medi apa           31         Apache CXF 2.7.2 (Apache 2.0)         3 - Medi apa           32         Apache CXF 2.5.2 (Apache 2.0)         3 - Medi apa	che Name s	Apache Cassandra 1.1.0 (Apache 2.0)					
33 Apache CXF 2.5.8 (Apache 2.0) 3 - Medi apa 10 Apache DirectMemory Cache 0.6.0 3 - Medi apa	che Owner	Auto-WriteUp (Palamida)					
<ol> <li>Apache Geronimo Java EE Specific 3 - Med apa</li> <li>Apache HitpComponents HitpClien 3 - Med apa</li> <li>Apache HitpComponents HitpClien 3 - Med apa</li> <li>Apache HitpComponents HitpCore 3 - Med apa</li> </ol>	che Description	The Apache Cassandra database is the right choice when you need scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability without compromising performance of the scalability and high availability					
les Namespace	Nc URL	http://cassandra.apadhe.org/					
	Su	Status Priority Shipped Modified Remediation Field of Use					
intire Workspace 👻	Component	In Progress • 3 - Medum • Unknown • No • apache-cassandra • • Version 1.1					
8- 🛄 C:\Demo1 🔹	Selected License	Apache License 2.0					
	Possible Licenses	Apache License 2.0					
	As-Found License Text	Sample from LICENSE tut in flie cassandra-all-1.1.0.jar in the materials: Agache License Version 2.0, January 2004 http://www.aduk-cogil.comves/					
		TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions.					
		"License" shall mean the terms and conditions for use, reproduction,					
e Count : 419	External Notes	Sample from NOTICE:tot in fle cassandra-uil-1.1.0.jar in the materials: Apache Cassandra Copyright 2009, 2010 The Apache Software Foundation					
		This product includes software developed by The Apache Software					

After reviewing the results, the auditor can publish the groups to create project inventory.

### Enabling Auto-WriteUp™

Auto-WriteUp<sup>™</sup> can be enabled or disabled as part of the **Workspace Settings** before scheduling a scan.

🚱 Home 🛛 🥥 Administration 👻 🕼 My Proj	acts   🚦 Policies   📎 Scheduler   🟮 Research   📨 Reports 🦳 Welcome admin   🌄 My Settings   🤣 Help   🖏 Logout
$\bigcirc$ Project1 $\rightarrow$ Workspace $\rightarrow$ Workspace1	Settings
General Detection Source Code Options	Rescan Options Automated Analysis
Enable POM File Analyzer	<u>E</u>
Enable Auto-WriteUp	
Enable Release File Detector	
Enable Multi-Indicator Detector	
Enable Release Coverage Detector	Minimum Threshold 0.0 (enter a value between 0.0 and 1.0)
Enable Point Detectors	
Add Non-Indicator Files to Groups?	
	Save Cancel

### **Detection Rules**

The Auto-WriteUp<sup>™</sup> engine is driven by detection rules and updated weekly via the Electronic Update Service.

- FlexNet Code Insight Rules
- High-Volume Rules
- User Defined Rules

#### **FlexNet Code Insight Rules**

Rules created manually by FlexNet Code Insight analysts are called FlexNet Code Insight Rules. These rules can be created for virtually any component which contains unique releases. After a component is thoroughly researched, its rules will contain licensing information, any pertinent auditor notes, and any envelope issues (described in the next section).

#### **High-Volume Rules**

A forge is a repository of OSS software, typically a web site or an FTP site. For example, some popular forges include GitHub (http://www.github.com), SourceForge (http://www.sourceforge.com), and GNU (http://ftp.gnu.org/).

High-Volume Rules are created automatically by downloading available releases and associated metadata from a forge. Unlike manually created FlexNet Code Insight Rules, High-Volume Rules only contain information that is available from the forge, which typically does not include information about envelope issues or auditors notes.

#### **User Defined Rules**

Starting with version 6.6.1 of FlexNet Code Insight, users can define custom detection rules. To create custom Auto-WriteUp™ rules, contact your FlexNet Code Insight account representative to set up a training session.

## **Configuring Auto-WriteUp™**

Auto-WriteUp<sup>™</sup> configuration is stored in the following location on the FlexNet Code Insight Core Server:

<code\_insight\_install\_dir>/config/core/Auto-WriteUp.properties

The following properties are supported:

Name	Value					
groupOptions	A comma-separated list of any of the following options (including no options):					
	• DO_VER					
	• DO_ENV					
	SET_PRI					
	• REF_PARENT_VER					
maxHeaders	<integer></integer>					
useShortText	true/false					
autoPublish	ALL_GROUPS/CODE_INSIGHT_GROUPS/COMPLETE_GROUPS					
userRules	A comma separated list of file names or <no value="">.</no>					

*Important* • Contact Flexera Software Support (https://flexeracommunity.force.com/customer/CCContactSupport) before editing the configuration file. Incorrect values may result in errors and a failed scan.

#### **Property Definitions**

The following are property definitions for Auto-WriteUp's supported properties.

Property	Description	
<b>groupOptions</b> (comma separated list)	SET_PRI	Automatically assign priorities to groups created by Auto-WriteUp™. The following priorities are supported based on the license or set of licenses associated with the group:
		• <b>P1</b> : Known copyleft OSS licenses (such as GPL, LGPL, MPL).
		• <b>P2</b> : Unknown, proprietary, commercial, or modified licenses.
		• <b>P3</b> : Known permissive OSS licenses (such as Apache, MIT, BSD).
	DO_VER	Create groups based on the component, version, and license of detected OSS content. When this option is omitted, Auto-WriteUp™ will group files based on the component and license only.
	DO_ENV	Create separate groups for envelope issues. Envelope issues (also known as embedded issues) are separate third- party content inside a parent component. Typically the third- party component is compiled, packaged, or copied inside the parent component (not to be confused with static or dynamic dependency linking). Envelope issues can be especially important if the third- party component is licensed differently than the parent component.
	REF_PARENT_VER	Explicitly reference the version of the parent group when creating envelope groups. This option has no effect if the DO_ENV or the DO_VER options are omitted.
<b>maxHeaders</b> (integer, default: 3)	r of headers to use when providing evidence for a the As-Found-License-Text field of a group in the etector Client. Typically, a single header refers to a nned code base.	
<b>useShortText</b> (true/false, default: true)	full license text when p	se a short sample of the license text instead of the opulating the As-Found-License-Text field of a ode Insight Detector Client.

Property	Description						
autoPublish (ALL_GROUPS/FlexNet Code	Specifies which groups will be published if the Auto-Publish System- Detected Inventory is enabled in the Project Details.						
nsight_GROUPS/ COMPLETE_GROUPS, default:	ALL_GROUPS	Publish all groups created by Auto-WriteUp.					
COMPLETE_GROUPS)	FlexNet Code Insight_GROUPS	Publish all groups created by FlexNet Code Insight Rules.					
	COMPLETE_GROUPS	Publish any groups which contain licensing information (all groups created by FlexNet Code Insight Rules and a portion of groups created by auto-generated High-Volume Rules will contain licensing information).					
<b>userRules</b> (comma separated list)	A list of file names indicating which user-specified detection rules to before scanning. This property may be left blank if no user-specified are present.						
	the following directory o	ion rules are saved in Microsoft® Excel® workbooks to ry on the FlexNet Code Insight Core Server: call_dir>/config/core/rules/					

### **Frequently Asked Questions**

The following questions are often asked about FlexNet Code Insight Auto-WriteUp:

- How are Auto-WriteUp™, FlexNet Code Insight Rules or High-Volume Rules Groups Marked?
- How can I tell which files were detected by Auto-WriteUp™?
- Why did Auto-WriteUp<sup>™</sup> create duplicate groups?
- Why did Auto-WriteUp<sup>™</sup> create groups with unpopulated fields?
- Why did Auto-WriteUp<sup>™</sup> create groups without versions though I included the DO\_VER option in the Auto-WriteUp<sup>™</sup> configuration?
- How can I tell if a group contains envelope issues without creating envelope groups?
- After editing an Auto-WriteUp<sup>™</sup> group, will I lose the changes if I rescan the workspace?

#### How are Auto-WriteUp<sup>™</sup>, FlexNet Code Insight Rules or High-Volume Rules Groups Marked?

Each group created by Auto-WriteUp<sup>™</sup> is marked as a System group. The **Owner** column in the FlexNet Code Insight Detector Client lists the forge associated with the group. The FlexNet Code Insight forge indicates a group was created with rules manually verified by FlexNet Code Insight analysts. Other forges indicate the group was created by auto- generated High-Volume Rules.

Workspace Script About													
Welcome Groups Tags	Filters Compo	nents Licenses	Emails/Urls Se	earch Terms Copy	rights								
		Select All	Clear All	Publish	Recal 🗍 🕅 I	gnored	V	Emp	ty				
Name	Priority	Component /	License	Owner	System					sł	nipped		
ASM [bundled with MV	3 - Medium	asm-framework	BSD 3-clause	Palamida	Yes	0	No	In	U l	J Un	known	1	1 /
atinject 1 (Apache 2.0)	3 - Medium	atinject	Apache Lice	Palamida	Yes	0	No	In	U L	J Un	known	2	2
BeanShell 2.0 (LGPL or	1 - Critical	beanshell-proj		Palamida	Yes	0	No	In	U l	J Un	known	1	1
berkeleydb 1.5.1	6 - Not Set	berkeleydb		Ibiblio Maven2	Yes	0	No	In	U l	J Un	known	1	1
berkeleydb 1.5.0	6 - Not Set	berkeleydb		Ibiblio Maven2	Yes	0	No	In	U l	J Un	known	1	1
berkeleydb-native 4.2	6 - Not Set	berkeleydb-na		Ibiblio Maven2	Yes	0	No	In	U l	J Un	known	1	1
Bouncy Castle Crypto	3 - Medium	bouncycastle	Legion Of Th	Palamida	Yes	0	No	In	U l	J Un	known	1	1_
cglib 2.2.3 (Apache 2.0)	3 - Medium	cglib	Apache Lice	Palamida	Yes	0	No	In	U l	J Un	known	1	1
cglib 3.0 (Apache 2.0)	3 - Medium	calib	Apache Lice	Palamida	Yes	0	No	In	U l	J Uni	known	1	1

Each group has information in the **Detection Notes** field that describes the rules used to create the group.

Detection Notes	Detected by Palamida Auto-WriteUp.	١١
	Generated from Ibiblo Maven2, see URL (http://mirrors.ibiblio.org/maven2/berkeleydb/berkeleydb).	
	Save	

#### How can I tell which files were detected by Auto-WriteUp™?

Files detected by Auto-WriteUp<sup>™</sup> have a Detection Evidence tag indicating they were detected by Auto-WriteUp<sup>™</sup>.

	acb71858391b35b831370d64b7934		
Summary Exact Matches Partial M	atches Tags Groups		
Name /	Value	System	
Contains No Indicators	Yes	Yes	
Detection Evidence	Detected by Auto-WriteUp (Palamida	i) Yes	
In Group	Yes	Yes	

#### Why did Auto-WriteUp™ create duplicate groups?

Auto-WriteUp<sup>™</sup> does not create duplicate groups. However duplicate components may exist on forges. In that case it may appear that Auto-WriteUp<sup>™</sup> created duplicate groups.

#### Why did Auto-WriteUp<sup>™</sup> create groups with unpopulated fields?

Groups created from FlexNet Code Insight Rules will always be filled out. Groups created from auto-generated High-Volume Rules include as much (or as little) information as can be gathered from the forge associated with the group.

## Why did Auto-WriteUp<sup>™</sup> create groups without versions though I included the DO\_VER option in the Auto-WriteUp<sup>™</sup> configuration?

Not all rules can be associated with appropriate versions.

#### How can I tell if a group contains envelope issues without creating envelope groups?

The External Notes field of the group will contain information about any embedded issues.

#### After editing an Auto-WriteUp<sup>™</sup> group, will I lose the changes if I rescan the workspace?

No, Auto-WriteUp<sup>™</sup> will not remove any changes to the group as part of a rescan.

### Workspace Backup/Restore Scripts

If you plan to use the workspace backup and restore Groovy scripts with Auto-WriteUp<sup>™</sup>, contact Support (https:// flexeracommunity.force.com/customer/CCContactSupport) to discuss how they interact.

### Troubleshooting

FlexNet Code Insight Auto-WriteUp has the following troubleshooting topics:

- How do I know if an error occurred when Auto-WriteUp<sup>™</sup> was running?
- If an error occurs when Auto-WriteUp™ is running, does the entire scan fail?
- Why are changes to the Auto-WriteUp.properties file not reflected after running a new scan?

#### How do I know if an error occurred when Auto-WriteUp<sup>™</sup> was running?

The Scheduler Task History will report the scan as having failed. Auto-WriteUp<sup>™</sup> will log all errors to <Code\_Insight\_install\_dir>/logs/Auto-WriteUp.log.X files. If Auto-WriteUp<sup>™</sup> is unable to start, errors will be logged to the Tomcat stdout facility.

🚱 Home   🎲 Administra	tion 👻   🧭 My Projects   🔋 1	Policies   🕑 Scheduler   🚷	Research   🔀 Repor	ts Welcome admin	🇞 My Settings   🤣 Help   🍕 Logout
Scheduler					
Scan Server: Scanner1		*			
Task Queue Task His	tory				
Filter: Tasks Completed La	ast Week 🗸 🗸				
Workspace	Project	Task Started	Task Completed -	Task Type	Task Status
Workspace1	Project1	06/05/2014 01:46	06/05/2014 01:48	Scan	Failed

#### If an error occurs when Auto-WriteUp™ is running, does the entire scan fail?

No, although the Scheduler Task History displays the scan status as failed, the scan results were committed before Auto-WriteUp<sup>™</sup> was invoked.

## Why are changes to the Auto-WriteUp.properties file not reflected after running a new scan?

When Auto-WriteUp<sup>™</sup> runs for the first time on any workspace in a project, it saves its configuration to the project metadata. Subsequent rescans on any workspace in that project will read the configuration from the project metadata. It is currently not possible to run Auto-WriteUp<sup>™</sup> with the new configuration without deleting all Auto-WriteUp<sup>™</sup> groups from all workspaces in that project.

**Chapter 21 Using Auto-WriteUp™** Frequently Asked Questions



# Workspace Scanning & Report Scheduling

Information about performing a workspace scan and scheduling reports is presented in the following sections.

- Scheduling a Scan
- Generating a Report

## **Scheduling a Scan**

To schedule a scan or generate a report, perform the following steps.

Task	To schedule a scan:					
	<b>1.</b> Log in to FlexNet Code Insight as the <b>Auditor</b> .					

- 2. Select the My Projects tab.
- 3. Choose a project, and click the project name or the associated Magnifying Glass icon in the Action column.
- 4. Click the Workspaces tab.

🕯 Home   🧭 My Projects	Policies	Schedu	ler   🔒	Research	Reports	Welcome A	Auditor   🏖 My Settings   🛟 Help   🐗 Logo
🕽 ePortal 1.3 (Enterprise	portal applica	tion, version	1.3.)				
Summary Workspaces	Inventory	Requests	Tasks	Policies	Comments		
Search:			\$	D			• Create New Workspace
Name 🔺		Server			Audit Progress		Actions
ePortal_13	1	server1				12 of 43 files with indicators reviewed 6 of 35 files without indicators reviewed	Q 🔅 🛇 🌌 🜹
4 4   Page 1 of 1	► N   2	Show All					1 - 1 of 1

5. Click the name of the workspace link in the **Name** column or the associated Magnifying Glass icon in the Action column that you wish to scan. The Workspace Details page appears.

© ePortal 1.3 → Work	sspace → ePortal_13
Schedule Scan/Repor	t 🛛 🗔 Workspace Resources 🔻 🛛 🐻 Workspace Operations 🔻
Name	ePortal_13
Server	server1
Created On	08/10/2011 13:03
Last Scanned	08/10/2011 13:28
Audit Progress	12 of 43 files with indicators reviewed         6 of 35 files without indicators reviewed
	Ok

6. From the Workspace Details page, click Schedule Scan/Report. A list of available reports appears:

1	Name 🔺
V	File Evidence Map Report
1	Forensic Data-Copyright Matches
V	Forensic Data-File Matches
V	Forensic Data-Namespace Matches
1	Forensic Data-Scan
V	Forensic Data-Search Term Matches
7	Forensic Data-Source Code Matches
V	License Detection Evidence Report
V	Scanned Files Report
1	Third-Party Indicators Report

- 7. Select the reports that you want to generate after the scan completes, and then click the Scan + Report button.
- 8. To schedule a scan without reports, ensure all Report checkboxes are unchecked, and then click the Scan button.
- **9.** If you configured an SCM application for the current workspace, an SCM sync/update/checkout will be performed based on the selected SCM application. If the operation fails, the scan will be terminated.

**Note** • If ClearCase is installed, the selected view is started and the selected VOBs are mounted. If the operation fails, the scan is terminated.

See the *Installation and System Administration Guide* for detailed instruction related to SCM configuration for workspaces and project copy.

### **Generating a Report**

To generate a report, see Generating Reports.



# **Workspace Resources**

This section includes the following topics:

- Accessing Workspace Resources
- Editing Workspace Settings
- Launching Detector
- Viewing Tasks in Queue for a Workspace
- Viewing Reports for a Workspace

### **Accessing Workspace Resources**

To access workspace resources, perform the following steps.

# Task

#### To access workspace resources, do the following:

- 1. Log in to FlexNet Code Insight as the Auditor.
- 2. Select the My Projects tab.
- 3. Choose a project, and click the project name or the associated Magnifying Glass icon in the Action column.
- 4. Select the Workspaces tab to open the Project Workspace view.
- 5. Click the Workspace Resources button and select one of the following:
  - Editing Workspace Settings
  - Launching Detector (after scheduling a scan)
  - Viewing Tasks in Queue for a Workspace
  - Viewing Reports for a Workspace.

## **Editing Workspace Settings**

To edit a workspace, do the following:

Task

To edit a workspace, do one of the following:

- From the Workspace Resources pull-down, select Edit Workspace Settings.
- Click the Cog icon that corresponds to the workspace.

Note • The Workspace Details setting is the Magnifying glass icon.

## **Launching Detector**

To launch Detector, perform the following steps.

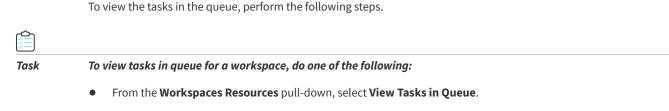


Click the Monitor icon that corresponds to the workspace.



**Note** • The first time that you launch Detector on a new client machine, you will be prompted to trust a JAR file from The Legion of the Bouncy Castle (http://www.bouncycastle.org/). Check the checkbox **Always trust content from this publisher**, then click **Run** to accept. This is an expected event and should only occur once.

## Viewing Tasks in Queue for a Workspace



Click the Clock icon that corresponds to the workspace.

# **Viewing Reports for a Workspace**

To view reports, perform the following steps.

Task	

To view reports, do one of the following:

- From the Workspaces Resources pull-down, select View Reports.
- Click the **Graph** icon that corresponds to the workspace.

Chapter 23 Workspace Resources

Viewing Reports for a Workspace



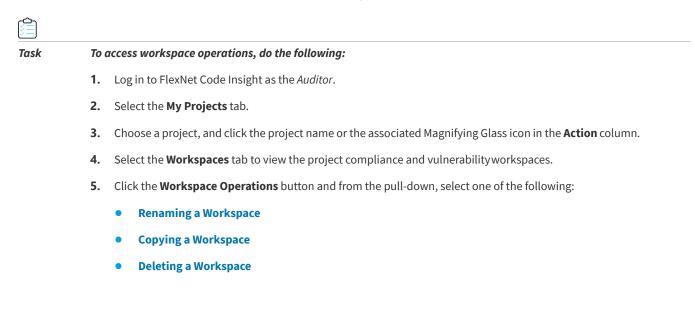
# **Workspace Operations**

Workspace operations include the following:

- Accessing Workspace Operations
- Renaming a Workspace
- Copying a Workspace
- Deleting a Workspace

## **Accessing Workspace Operations**

To access workspace operations, perform the following steps.



## **Renaming a Workspace**

To rename a workspace, perform the following steps.

# Task

To rename a workspace, do the following:

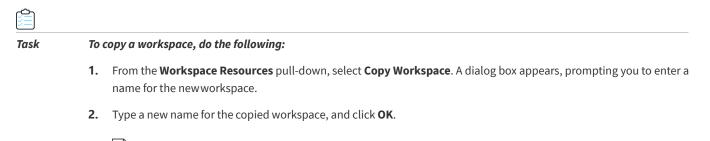
- 1. From the **Workspace Operations** pull-down, select **Rename Workspace**. A dialog box appears, prompting you to enter a new name for the workspace.
- 2. Type a new name, and click OK.



Note • Only letters, numbers, underscores, and dashes can be used in the workspace name.

## **Copying a Workspace**

To copy a workspace, perform the following steps.



Note • Only letters, numbers, underscores, and dashes may be used in the workspace name.

## **Deleting a Workspace**

To delete a workspace, perform the following steps.



To delete a workspace, do the following:

- 1. From the **Workspace Resources** pull-down, select **Delete Workspace**. A dialog box appears, prompting you to confirm that this is the workspace you want todelete.
- 2. Click OK to delete the workspace.



# **Using the Analyzer**

This section contains the following topics:

- The Analyzer
- FlexNet Code Insight Data Services
- Frequently Asked Questions

## **The Analyzer**

The Analyzer aids the auditing of third-party code by automatically identifying dependencies, packages, and source distributions. The Analyzer can be run at the following times:

- Before a scan task to get an overview of the contents of your codebase.
- After a scan to create component groups/inventory items.

The Analyzer provides the following functionality:

- Builds notices for groups/inventory items where possible to make creating third-party notices easier.
- Support for Composer (php) packages. If there is a composer.lock file, those defined dependencies and versions will be used. If there is no lockfile (for example, if the package has not been installed), composer.json files are parsed for uninstalled 'required' dependencies and the versions are set to the most recent version in the Packagist registry that satisfies the given composer.json's semantic versioning restrictions.
- Support for npm uninstalled node modules. Inventory items are created when there is a package.json with dependencies even when the corresponding node modules are not present. The npm Analyzer uses the npm registry to get package information and resolve semantic versioning. Versions are set to the most recent version in the npm registry that satisfies the semantic versioning restrictions in the given package.jsonfile.
- Support for Tomcat webapps rebranding. There are webapps named codeInsightScanner and palamidaScanEngine. The update jar can be used in Flexnet Code Insight versions 6.10.3+.

### Requirements

The following are requirements to run the Analyzer:

- The Analyzer must be enabled on the Automated Analysis tab. See Automated Analysis Tab for details.
- A FlexNet Code Insight Data Services-enabled key is required to enable the Analyzer to query FlexNet Code Insight Data Services' open source data library using HTTPS GET requests. If you require a new key, contact Flexera technical support: https://flexeracommunity.force.com/customer/CCContactSupport.

## Reports

Workspace reports include the following:

- Analyzer--Quick Assessment creates an html report of Analyzer findings.
- Analyzer--Group Builder creates an html report and creates groups in your project.

## Permissions

The project owner and project auditor roles can run the Analyzer workspace tasks and view the resulting reports.

## **Running the Analyzer**

Task

To run the Analyzer, do the following:

1. Click the Schedule/Scan Report button in the Workspace.

ace -+ libw	Schedule Scan/Report	
🕄 Workspace Rese	Name +	
libw	Forensis Data-File Matches Forensis Data-Namespace Matches	
Scan_franklin	Forensic Data-Scan	
08/24/2016 1;	Forensic Data-Search Term Matches	
08/24/2016 11		
	Palamida Analyzer - Group Builder	
	Patamida Analyzer - Guick Assessment Scanned Files Report	
8.10.0	Third-Party Indicators Report Vorkspace Evidence Report	
	libw Scan_franklin 08/24/2016 1:	Name A     Norme A     No

2. To run the Quick Assessment, run as a **REPORT only** (not in conjunction with a scan).



**Note** • The Analyzer will not do an SCM pull before analysis, though. SCM pulls are only done at scan time or can be triggered manually.

The Group Builder should only be run **after a scan**. You can select this task at the same time you kick off a scan or wait until the scan is complete. Just as with a scan, it is recommended to close all Detector client windows before running.

# **FlexNet Code Insight Data Services**

FlexNet Code Insight Data Services is a RESTful API hosted on Amazon Web Services. Data Services provides information about Open Source projects from the FlexNet Code Insight Data Library. Queries can be made against the following entities:

- Components: open source projects and their metadata (URL, description, licenses, etc)
- Versions: the version names of components, vulnerabilities, per-version licenses, etc.
- Licenses: text, whether it is copyleft or compatible with versions of the GPL, etc.)
- Vulnerabilities: CVE, CPE info, scores, etc.)
- Digests: exact md5 digest matches, auto-writeup rules, etc.

Requests to Data Services take the form of an HTTPS GET request to the web service. The following typical query is a request for the names of the licenses associated to FlexNet Code Insight components with the name 'zlib':

/components?fields=component\_license\_names&query=name:zlib

The Analyzer is the first application built to use DATA SERVICES. The Analyzer does a combination of file parsing, built-in component analysis, intelligent reading of typical metadata sources (package.json, pom.xml, etc.), and queries to DATA SERVICES and other web services to create an open source inventory. DATA SERVICES supplements license information, component metadata, and known security vulnerabilities.



**Important** • Files and code snippets are never sent to DATA SERVICES, which is queried only for information about Open Source projects as contained in the FlexNet Code Insight Data Library (e.g., component information, vulnerabilities, licenses, digest-to-component data) to enable rich inventory building.

### Ports

The Analyzer requires outgoing TCP access on port 443. Proxy support can be enabled in analyzer.properties.

### Setup

Ensure you have a Data Services-enabled key file (palamida.key or codeinsight.key), which is all that is required to use the Analyzer. Restart Tomcat if you are replacing an existing key. For an example of additional properties that may be configured, see <CODE INSIGHT ROOT>/config/core/analyzer.properties.example.

- 1. Copy the example file to <CODE\_INSIGHT\_ROOT>/config/core/analyzer.properties.
- 2. Restart Tomcat to try the configuration.

## Performing a Quick Assessment with the Analyzer

You can use the Analyzer to perform a quick assessment of your project. The analyzer Quick assessment report can be run on any project in a workspace. The workspace does not need to be scanned to run the report.

Š=		
Task	То ј	perform a quick assessment, do the following:
	1.	Sign into FlexNet Code Insight.
	2.	Select My project.
	3.	Select <b>My workspace</b> .
	4.	Click Schedule Scan/Report.
	5.	Click Analyzer – Quick Assessment from the menu.
	6.	Click <b>Report</b> to generate a report based on the unscanned workspace.
	7.	To access the report, select View Reports from the Workspace Resources menu. A list of generated reports appears.

8. Select the Analyzer - Quick Assessment report from the list.

## Auto-creating Component Groups with the Analyzer

The analyzer Group builder is a task that runs on a project workspace during or after a scan task. This task can be run on any workspace. The task runs on the following:

- The scan results produced by the scanner.
- File contents for the scanned files of interest.

# Task

### To auto-create component groups, do the following:

- 1. Sign into FlexNet Code Insight.
- 2. Select My project.
- 3. Select My workspace.
- 4. Click Schedule Scan/Report.
- 5. Click Analyzer Group Builder from the menu.
- 6. Click **Report** to generate a report based on the workspace.
- 7. To access the report, select View Reports from the Workspace Resources menu. A list of generated reports appears.
- 8. Select the Analyzer Group Builder report from the list.

## Administration

The Analyzer requires a new key file (palamida.key or codeinsight.key) to enable access to FlexNet Code Insight Data Services. If you use your old key, the workspace reports will fail. If your FlexNet Code Insight server does not have internet access, you can turn off Data Services in analyzer.properties to apply limited analysis techniques.

The feature is enabled by default for all projects, but it can be globally disabled or enabled for specific projects. Contact Support at https://flexeracommunity.force.com/customer/CCContactSupport to enable admin mode to turn off the Analyzer selectively.

The feature can be configured to run automatically with each scan without selecting the **Analyzer - Group Builder** report. Contact Support at https://flexeracommunity.force.com/customer/CCContactSupport for instructions.

### **Updates**

When the report task runs on the scan server, it automatically downloads and installs the update jar from the core server. The Electronic Update includes the latest Analyzer update jar.

## Settings

System settings are controlled via a properties file on the core server in config/core/analyzer.properties. You can use the example file config/core/analyzer.properties.example to view the possible options and to create your own properties file.

## **Core Settings**

### **Analyzer Use Data Services**

Determines whether to use the FlexeNet Code Insight Data Services API for additional analysis techniques. The default is *true*.



Note • This requires a license key with Data Services enabled, and outgoing TCP access on port 443.

### **Analyzer Use RubyGems API**

Determines whether to use the RubyGems public API for additional analysis.



**Note** • This requires outgoing TCP access on port 443.

## **Project Settings**

Project settings are controlled via \*Yes/No\* Metadata fields. You can create these Metadata fields by running the configurePalamidaAnalyzer.groovy script, as above. The default values are controlled via analyzer.properties.

### **Analyzer Auto Schedule**

Whether to auto-schedule to the report task for enabled projects. The default is *true*. To change the default, set autoScheduleTask in analyzer.properties.

### **Analyzer Auto Include**

Whether to select "Include in Third-Party Notices" for the groups that the Analyzer creates. Groups will only be included if they have license text. The default is *true*. To change the default, set autoIncludeNotices in analyzer.properties.

### Analyzer Override MID rules

Whether the Analyzer should take files out of MID rule groups with the same component, and delete the groups if they are empty afterwards. The default is *false*. To change the default, set overrideMidrules in analyzer.properties.

### **Analyzer Resolve Transitive Dependencies**

Whether to include transitive dependencies. Currently this only affects the POM Analysis. The default is *true*. To change the default, set transitiveDependencies in analyzer.properties.

## **Frequently Asked Questions**

The following are questions that are often asked by FlexNet Code Insight users:

- How do I know if a group was created by the Analyzer?
- How do I know if a file has been analyzed by the Analyzer?
- How do I know what information the Analyzer used to create the group?
- Do I still have to audit and where should I start?
- Why do some groups have Unknown in the group name?
- What if the Analyzer finds a package that doesn't have a component?
- What happens to the Analyzer groups when you rescan a workspace?
- Does the Analyzer find vulnerabilities? How?
- Does the Analyzer do License Scanning/Copyright Detection/Source Code Fingerprint Analysis?
- Does the Analyzer mark files as reviewed?
- Why are my own Java modules or dependencies listed as inventory items?

### How do I know if a group was created by the Analyzer?

*Analyzer* or *Component Analyzer* will appear in the group's **Owner** field. The group will also have Detection Notes that say "Detected by Analyzer" along with some information about the analysis techniques used.

### How do I know if a file has been analyzed by the Analyzer?

Each file that the Analyzer places into a group receives a special tag of *Detection Evidence* with the value *Detected by Analyzer*. This tag can also be used in filters.

### How do I know what information the Analyzer used to create the group?

Take a look at the group's detection evidence to see what analysis techniques and data sources the Analyzer used.

### Do I still have to audit and where should I start?

The Analyzer is not intended to be a replacement for a good forensic open source audit. As always, you should decide what the appropriate depth of audit is for each of your code projects. In most cases, at least some additional audit work is highly recommend. Some good starting places would be to:

- Identify groups with unknown or unexpected licenses and use the FlexeNet Code Insight scan results to identify/verify the license.
- Check for "envelope" issues (cases where a component declares a permissive license but contains code from or a dependency on a component under an unacceptable license). It is a good idea to check high priority scan evidence such as search terms indicative of a copyleft license.
- Mark files associated to Analyzer groups as *Reviewed*; and then proceed with your normal audit process to explain remaining instances of open source licenses, third party copyrights, and exact digest matches. You can easily find all the files within Analyzer groups by creating a Tag Value Expression filter on Detection Evidence which contains *Analyzer*.

### Why do some groups have Unknown in the group name?

The Analyzer uses a variety of techniques to try to determine the license of the inventory item. If none of the techniques pan out, the inventory item is marked *Unknown License*. For these items, the usual audit techniques should be applied in the Detector client to ascertain the license (if there is one).

### What if the Analyzer finds a package that doesn't have a component?

The Analyzer will try a variety of techniques to find a component match for the group, but if it does not that field and the version field will be left blank. If you would like to add a component to the Data Library, contact Library-Request@Flexeerasoftware.com.

### What happens to the Analyzer groups when you rescan a workspace?

The Analyzer will not delete any groups from the previous scan. New groups will be created as appropriate. You can sort the Groups list in Detector to see which groups were recently created/updated. Consider deleting the old groups unless you have made changes to them.

### Does the Analyzer find vulnerabilities? How?

The Analyzer is not a vulnerability scanner in the sense of software like Fortify. Rather, the Analyzer is able to identify Open Source projects in your code and use the FlexeNet Code Insight Data Library to see whether any of the projects have been mapped to known/published security vulnerabilities by the Library team. These curated mappings help reduce false positives that often result from pure text-based CVE lookups.

# Does the Analyzer do License Scanning/Copyright Detection/Source Code Fingerprint Analysis?

No, the Analyzer does not do systematic license detection. However, the Analyzer does use the license scanning data in the Group Building mode on some occasions and uses a variety of techniques to get license information, but it is not a replacement for the FlexeNet Code Insight scanner and a good audit. In general, the Analyzer should be used in conjunction with the standard auditing methods for the discovery of open source licenses in the Detector client.

### Does the Analyzer mark files as reviewed?

No, files should be marked as reviewed by an auditor when the depth of audit appropriate for the workspace has been completed. For some types of audit, it might be appropriate to mark the files as reviewed after a limited review for high-priority evidence types or envelope issues. For a more forensic audit, it might be appropriate to wait until more evidence has been evaluated (such as source code fingerprints).

### Why are my own Java modules or dependencies listed as inventory items?

Some customers find it useful to visualize and understand their project hierarchy by placing the dependencies in the context of the module they are part of. If you do not find these items to be useful, delete the groups in Detector or do not publish them as inventory items.



# Accessing a Workspace to Analyze

This section contains the following topic:

• Accessing Workspaces

# **Accessing Workspaces**

To schedule a scan and later analyze that scan, you need first to choose the workspace for which you want to analyze scan results.

📋 Task

### To choose a workspace, do the following:

- 1. Click the My Projects button.
- 2. Click the name of the project.
- 3. Click the Workspace tab.
- 4. Select a workspace to scan by clicking on the workspace link in the Name column.

Summary Works	spaces Invent	ory Requests	Tasks	Policies	Comments		
Search:			Q				Create New Works
Name 🔺		Server		Audit Pr	rogress		Actions
ePortal_13		server1				43 files with indicators reviewed 5 files without indicators reviewed	a 🌼 🛛 🚟 📮

5. Click the Schedule Scan/Report button. The Schedule/Scan Report dialog appears with a list of available reports to generate.

### Chapter 26 Accessing a Workspace to Analyze

Accessing Workspaces

- Schedule Scan/Report
   X

   V
   Name 4

   V
   File Evidence Map Report

   V
   Forensic Data-Copyright Matches

   V
   Forensic Data-Scane

   V
   License Detection Evidence Report

   V
   Third-Party Indicators Report

   Scan
   Report

   Scan
   Report
- 6. Click a specific report checkbox. You have the option to generate a report only or a scan and a report.



# Viewing and Updating Scheduler Queuing

This section contains the following topic:

• Viewing the Scheduler Queue

# Viewing the Scheduler Queue

To view the scheduler queue, perform the following steps.

۲ <u></u>	
Task	

#### To view the scheduler queue, do the following:

- 1. Click the Scheduler button in the Main menu.
- 2. Select a scan server from the Scan Server pull-down.

an Server:	Core Server		~			
Task Queu	Core Server					
i usk Quet	Scanner1					
Active Tas	k					
Project		None				
Workspa	ace	System				
Task Typ	pe	Electronic Update				
Added to	o Queue at	08/28/2014 15:58 by	8/2014 15:58 by palamida palamida			
Started I	arted Execution at 08/28/201		15:58			
Status		Waiting for scan task	to f	inish before starting Electronic Update		
Pendina T	asks (drag tasks	to reorder queue)				
		s for this scan server.				

**3.** You can schedule as many scans as you wish. To prioritize a certain scan, hover over the boxed-in number in the right column and drag and drop the scan to a different position.

- **4.** To move a scan up or down in completion priority, select the scan or report numbers and drag it to the spot you wish it to occupy in the list. You can also cancel a scan by clicking the red X icon. This feature allows you to maximize your time auditing because you don't have to wait for a scan to finish, just reorder the scan priorities.
- 5. The queue list automatically renumbers as you drag and drop the task into position. You can also click **Refresh Page** to refresh the page.
- 6. Select the Task History tab to view the time a task started and completed, as well as the task type and status.

an Server: server1		*			
Task Queue Task Hist	ory				
Workspace	Project	Task Started	Task Completed -	Task Type	Task Status
ePortal_13	ePortal 1.3	08/10/2011 13:28	08/10/2011 13:33	Report - File Evidence Map Report	Completed
ePortal_13	ePortal 1.3	08/10/2011 13:28	08/10/2011 13:28	Report - Scanned Files Report	Completed
ePortal_13	ePortal 1.3	08/10/2011 13:28	08/10/2011 13:28	Report - Third-Party Indicators Report	Completed
ePortal 13	ePortal 1.3	08/10/2011 13:12	08/10/2011 13:28	Scan	Completed

$\mathbf{O}$
0

# Launching Detector & Viewing Scan Results

This section contains the following topics:

- Opening Detector to View Scan Results
- Detector Tabs and File Tree Views

# **Opening Detector to View Scan Results**

To open a workspace scan and analyze the code base before viewing the scan results, you must schedule a scan.



Note • For more information on scheduling a scan, see Scheduling a Scan.

To view scan results in **Detector**, perform the following steps.



2. The workspace opens automatically when you launch Detector.

Welcome Groups Tags Filters Components License	s Emails/Urls Search Terms Copyrights	
Files Namespace	No file or namespace selected.	<b>= = </b>
	Summary	
Entire Workspace		
⊕- 🔄 downloads ⊕- 🔄 embedded ⊕- 🔄 lib		
ierring src ierring web		
▼ ●		
File Count : 2431 Selected Items : 0		

## **Detector Tabs and File Tree Views**

Clicking on the tabs in the upper pane of Detector allow you to access summary data related to lastscan results. This includes project inventory and file counts for various third-party indicators.

Click the Plus (+) icon to the left of the folder icon in the lower pane **Files** tab file tree to expand the tree.

Files Namespace	No file or namespace selected.
	Summary
Entire Workspace	
Entire Workspace cs\tutorial\ePortal-1.	
Last Group Filter Last Tag Filter	
Last Custom Filter	
Last Component Filter	
Last License Filter	
Last Email/Url Filter	
Last Search Term Filter	
Last Copyright Filter	
Matched Java Names	
Unmatched Java Names	
Last Custom Script Filter	
<b>T</b>	
4	
File Count : 2431 Selected Items : 0	

There are several tree manipulation buttons above the file tree.

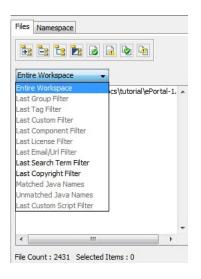
#### Table 28-1 • Tree Manipulation Buttons

Button	Description
÷	Expands the tree hierarchy.
	Collapses the file tree.

### Table 28-1 • Tree Manipulation Buttons

Button	Description
ĉ	Toggles between hierarchy and flat modes.
2	Allows you to view the inverse tree in hierarchy and flat mode.
D	Shows only reviewed files.
	Shows only unreviewed files.
	If the tree display is in flat mode, this button sorts the files in an ascending order.
<b>F</b>	If the tree display is in flat mode, this button sorts the files in a descending order.

The pull-down menu above the file tree allows you to apply a filter from recenthistory.



Chapter 28 Launching Detector & Viewing Scan Results

Detector Tabs and File Tree Views

5

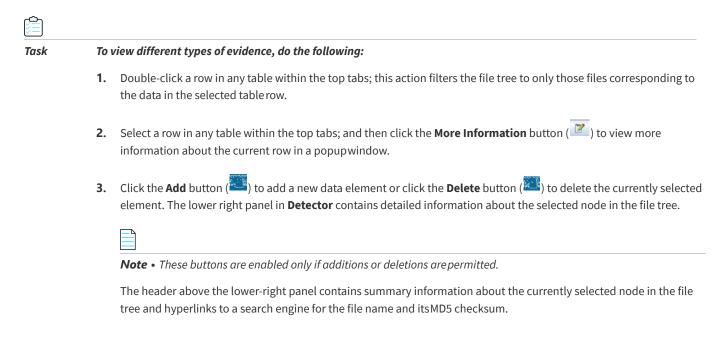
# **Viewing Evidence**

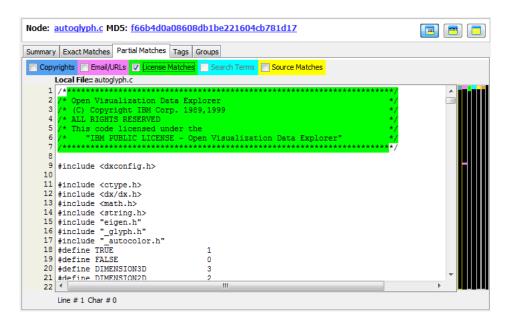
Information about viewing different types of evidence is presented in the following sections:

- Viewing Evidence
- Types of Evidence
- Filtering the File Tree
- Viewing SCM File Check-In History

# **Viewing Evidence**

After you open a workspace, you can view the tabs in the upper panel of Detector. They are named according to the types of information you can access via the scan.





## **Types of Evidence**

There are several types of third-party indicators available as part of the scan results. These include exact and partial file matches, copyrights, emails and/or URLs, license matches, source code matches, and custom search term matches. You may also choose to ignore copyrights, emails, and URLs if in the Properties file you define the elements you wish the system to ignore. Selecting a node in the file tree shows the file details in the bottom-right panel in Detector. The display consists of a node header as shown in Types of Evidence, and the following tabs (if appropriate):

- Summary
- Exact Matches
- Partial Matches
- Ignoring Copyrights, Emails, and URLs
- Tags
- Groups

### Summary

This tab contains file-level details about the currently selected node in the file tree.

### **Exact Matches**

This tab contains a list of components (including policy data if available) which holds a file, which is an exact (bit-for-bit) match with selected node in the file tree.

### **Partial Matches**

This tab contains various partial match details for the selected node in the file tree as shown in the four numbered sections in Tags.

- A set of checkboxes runs across the screen horizontally. These highlight various partial-match evidence examples in the selected node in the file tree, as do the following buttons.
- For Source Matches, a table with match details allows you to select which matches should be highlighted in the selected node in the file tree.
- This section contains the content of the selected node in the file tree on top of which highlights are shown.
- A set of color side bars corresponding to the evidence type checkboxes show the location of the highlights for each evidence type in the selected node in the file tree.

### Ignoring Copyrights, Emails, and URLs

In order to ignore copyrights, emails, and URLs, you must set up the strings you wish to ignore in the following properties files: Copyrights (ignoredCopyrights.txt), emails/URLs (ignoredEmailURL.txt). Both files are located in <CODE\_INSIGHT\_ROOT\_DIR>/6.13.x/config/scanEngine/. In effect, the system will not flag those elements you set it to ignore. This file may be used to force the scanner to skip a detected email/URL.

- The purpose of getting Detector to ignore one of these elements is so you can treat a file as if it does not have thirdparty content if it only has an internal email or URL within a String literal or comment.
- Lines beginning with # and blank lines are ignored.
- Each line is treated as a string to match. (There is no regex supported).
- An email or URL is ignored if it contains any of the strings from this file.
- The comparison is case-insensitive.
- Avoid use of strings that are over 100 characters in length and those that have hyphens in the name.
- To ignore a set of URLs with a similar pattern, it is recommended that you generalize the notation when possible. For example, to ignore the following five URLs you should use the pattern ://connect.palamida.com instead of listing each URL individually.

http://connect.palamida.com/EnterpriseEdition/release/details/304958/problem-with-treeviewdoubleclick-event

http://connect.palamida.com/EnterpriseEdition/release/details/367247/elementhost-set-childdoesnt-stop-listen

https://connect.palamida.com/EnterpriseEdition/release/details/

https://connect.palamida.com/EnterpriseEdition/release/details/694400

https://connect.palamida.com/EnterpriseEdition/release/details/719443/c-chrono-headers-highresolution-clock-d

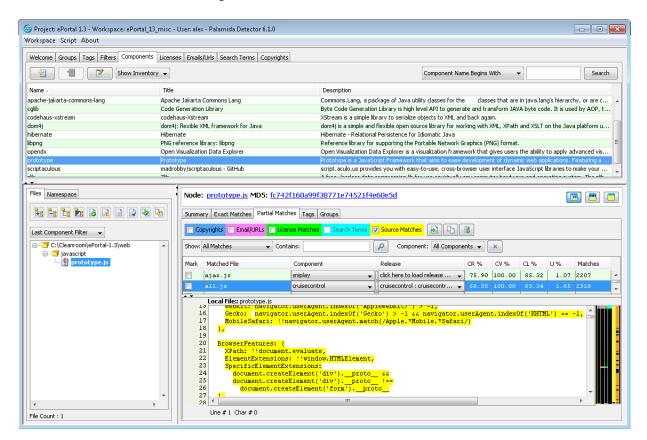
• Likewise, to ignore a set of emails such as those listed below you should use the pattern @palamida.com instead of listing each entry individually.

alex@palamida.com

julia@palamida.com

devnull@palamida.com

**Note** • Although files that only contain ignored emails/URLs are not tagged as containing these, if you look at the file in Detector you see the supposedly ignored emails/URLs highlighted. This is because the highlighting function in Detector uses its own search rather than basing itself on scan results.



### Tags

This tab contains a list of tags applied to the currently selected node in the file tree.

### Groups

This tab contains a list of groups to which the currently selected node in the file tree has been added.

## **Filtering the File Tree**

Information about filtering the file tree is presented in the following sections:

- Displaying Only Desired Files (Nodes)
- Displaying Only Exact Matches
- Displaying Partial Matches

## **Displaying Only Desired Files (Nodes)**

To filter the file tree to display only those files containing a specific type of evidence, perform the following steps.

Task	То	To filter the file tree to display only desired files (nodes), do the following:						
	1.	Double-click a desired row in the <b>Tag</b> table on the <b>Tags</b> tab in <b>Detector</b> .						
	2.	Other filter options include double-clicking on a desired Component, License, Copyright, or Search Terms from the corresponding tabs in the top panel of <b>Detector</b> .						
		<b>Note</b> • See Custom Script-Based Filters for more information about Custom Groovy script-based filters you can develop for custom or complex filtering.						

## **Displaying Only Exact Matches**

To filter the file tree to display only exact matches, perform the following steps.

# Task To filter the file tree to display only exact matches, do the following:

- 1. Click the node in the file tree for which you wish to review exact file matches.
- 2. Select the **Exact Matches** tab in the **File Details** panel. This shows a list of components that include files that are an exact (bit-for-bit) match to the currently selected node in the file tree. Policy icons indicate the component policies that exist for eachrow.
- **3.** There are three action buttons below the table that allow you to remove a component from the list, add a component to the list, or ignore a particular match from the list.

Files Namespace	Node: <u>aceqi-security-1.0.7.jar</u> MD5: <u>355696bb2e3d3c9892543396271d4d79</u>	
	Summary Exact Matches Partial Matches Tags Groups	
Entire Workspace 🗸	Show: All Matches  Contains:	
E	Mark Component	
ter downloads	acegisecurity	
🖶 🛅 embedded	D brihaspati	
🕂 🖓 👘 🔄 👘	Camptocamp-geonetwork	
iacegi-security-1.0.7.jar	Cia	
🗈 ず cglib-nodep-2.1_3.jar		_
🕀 🕤 commons-beanutils-1.7.0.jar	Coadunation	
🕀 🕤 commons-codec-1.3.jar	🔲 📔 dhubler-sipxecs	=
i commons-io-1.4.jar	emforge	
⊕	geoserver	
	P geowebcache	
itextpdf-5.1.2.jar	jamviki	
⊕ Stream-1.1.2.jar		
zlib1.dll		
	🔲 🟴 kayveo	
	P leechonjava	
pom.xml	lingportal	
File Count : 83		

## **Displaying Partial Matches**

Information about filtering the file tree to display partial matches is presented in the following sections:

- Displaying Copyrights
- Displaying Emails & URLs
- Displaying License Matches
- Displaying Search Term Matches
- Displaying Source Code Fingerprint (SCF) Matches
- Displaying Source Code Fingerprint (SCF) Matches
- Displaying Java Name Matches



**Note** • For more information on how to control the sensitivity of copyright detection, see "Tuning Copyright Detection" in the FlexNet Code Insight Installation and System Administration Guide.

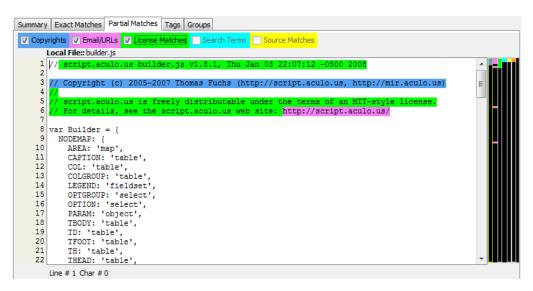
### **Displaying Copyrights**

To display copyrights, perform the following steps.

# Task

### To display copyrights, do the following:

- 1. A list of detected copyright holders is available in the **Copyrights** tab in the top panel in Detector.
- 2. Click the node in the file tree for which you wish to review detected copyrights.
- **3.** Select the **Partial Matches** tab in the file details panel and ensure that the **Copyrights** checkbox is checked to view the detected copyrights. Copyrights are highlighted in blue, and the corresponding vertical color bar to the right of the panel indicates matches which exist within the currently selected node in the file tree.



### **Displaying Emails & URLs**

To display emails and URLs, perform the following steps:

### Task

#### To display emails and URLs, do the following:

- 1. Click the node in the file tree for which you wish to review detected email addresses and URLs.
- 2. Click the Partial Matches tab in the file details panel and ensure that the Emails/URLs checkbox is checked in order to view the detected email addresses and URLs. Email addresses and URLs are highlighted in purple, and the corresponding vertical color bar to the right of the panel indicates the matches exist within the currently selected node in the filetree.

### **Ignoring Emails & URLs**

You can choose to ignore emails and URLS. To do this, include the email or URL you wish to ignore in the Properties file the same way you include copyrights to ignore.

### **Displaying License Matches**

To display license matches, perform the following steps.

#### Task

To display license matches, do the following:

- 1. Click the node in the file tree for which you wish to review detected license text and license references. Note that license matches are only highlighted in source files. Other file types are flagged (via tags) as containing license matches bug highlights within the partial matches tab, and are not available for non-source files.
- 2. Click the Partial Matches tab in the file details panel and ensure that the License Matches checkbox is checked to view the detected license text and license references. License matches (in source files only) are highlighted in green, and the corresponding vertical color bar to the right of the panel indicates matches which exist within the currently selected node in the file tree.

### **Displaying Search Term Matches**

To display search term matches, perform the following steps.

#### Task

#### To display search term matches, do the following:

- 1. Click the node in the file tree for which you want to review search terms.
- 2. Select the **Partial Matches** tab in the **File Details** panel and ensure that the **Search Terms** checkbox is checked to view the detected search terms. Search terms are highlighted in light blue, and the corresponding vertical color bar to the right of the panel indicates matches that exist in the currently selected node in the file tree.

### **Displaying Source Code Fingerprint (SCF) Matches**

Source code fingerprints are snippets within files that match content in source files found in third-party components. Source code fingerprints act as identifiers of likely third-party content within the scanned file.

To display source code fingerprint (SCF) matches, perform the following steps.

- 1. Click the node in the file tree for which you wish to review source codematches.
- 2. Select the **Partial Matches** tab in the file details panel and ensure that the **SCF Matches** checkbox is checked to view a list of third-party files for which there are source matches.
- **3.** Select a row in the matches table to highlight the currently selected node in the file tree with the source code matches that were detected from the selected remote file. The data in the table can be sorted by any of the columns. The following acronyms are used in the column headings to save space:
  - CR: Code Rank
  - CV: Coverage
  - CL: Clustering
  - U:Uniqueness
- **4.** Source code matches are highlighted in yellow, and the corresponding vertical color bar to the right of the panel indicates matches which exist within the currently selected node in the filetree.



**Note** • If you set sliders in the **Workspace Settings** page via Detector, only your local (on your machine and with your machine login only) scan results view will be affected. The sliders filter the file tree to display only those files that contain source matches above the defined thresholds. The list of source matches in the **Partial Matches** tab will not be filtered, so no scan results are hidden for a given file. When a file is selected from a complete scanned files tree of a filtered view, all source matches above the scan-source-match thresholds are shown in the source matchestable.

- 5. There are three buttons to the right of the Evidence Type checkboxes at the top of the Partial Matches tab.
- 6. To open the remote file from the selected Release (Component) in the source matches table in a local test editor, click



7. To open the remote file from the selected Release (Component) in a panel next to the scanned source file (dual-pane),

click . You can then review these two files side-by-side. You can perform text searches in either pane using the [Ctrl]+ [F] shortcut.

8. To load all source code matches, click . By default, only the first 500 matches are loaded. They are sorted in descending order by the number of matches they contain.

how:	All Matches	✓ Contains:	Component: All Components	
1ark	Matched File	Component	Release         CR %         CV %         CL %         U %	Matches
1	autoglyph.c	opendx	🗸 🕅 🏴 opendx : dx-4.2.0.tar.gz 🗸 🖌 87.35 100.00 53.77 100.00	0 159
1	glyph.c	opendx	dick here to load release data	0 151
1	glyph.c	opendx	✓ dick here to load release data	0 22
•	Local File:: autoglyph	c		
149 146 147	6 t 7 cou	se type_string[count] unt++;	<pre>= type_string[i];</pre>	
146	6 to the second	type_string[count] int++;	= ' ') (	

The File Details Panel Partial Matches tab with SCF Matches Dual-Pane View view appears:

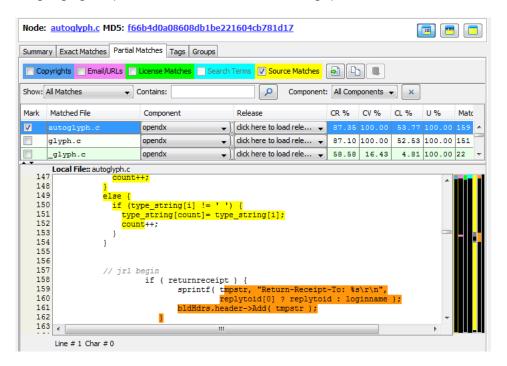
ow: All Matches 👻 Contains:	Compo	onent: All Components 👻 🗙					
ark Matched File	Component	Release	CR %	CV %	CL %	υ%	Matches
autoglyph.c	opendx 🗸	[ 🖫 opendx : dx-4.2.0.tar.gz 🛛 👻	87.35	100.00	53.77	100.00	159
glyph.c	opendx 👻	click here to load release data 💂	87.10	100.00	52.53	100.00	151
_glyph.c	opendx 🗸	click here to load release data 💂	58.58	16.43	4.81	100.00	22
_glyph.c	opendx 🗸	click here to load release data 💂	58.58	16.43	4.81	100.00	22
bldhdrs.cpp	blat 🗸	click here to load release data 💂	81.84	9.71	100.00	100.00	13
bldhdrs.cpp	blat 🗸	click here to load release data	81.81	8.96	100.00	100.00	12
Local File:: autoglyph.c		Remote File: autor	lunh c onondy i di	-4.2.0 tor. oz.			×
144         type_string           145         else           146         type_string           147         count+:           148         )           150         if (type_string)           151         type_string)           152         count+:           153         )           154         )           155         )           157         // jrl begin	<pre>p_string[i]) count]= tolower(type_string[ count]= type_string[i]; dg[i] != ' ') ( count]= type_string[i]; eturnreceipt ) ( sprint( tmpstr, "Return-Red replytoid[0] ? repl bldHdrs.header-&gt;Add( tmpstr Coby Korn tkorn@snl,com 8/4/1</pre>	<pre>i]);</pre>	<pre>i &lt; 29 &amp;&amp; typ (isalpha(type f (isupper(type type_string[ lse type_string[ ount++; e { f (type_string[ count++;</pre>	<pre>to lower case e_string[i] _string[i])) pe_string[i] count]= tolo count]= type g[i] != ' ') count]= type</pre>	!= '\0') { { wer(type_stri _string[i]; {	ng[i]);	▲ 138 139 140 141 142 143 144 145 147 148 148 148 148 148 148 148 150 151 152 153 154 155 155 155 155 155

### **Displaying Source Code Fingerprint (SCF) Matches**

Because a typical scanned source file may contain source matches from multiple origins, FlexNet Code Insight determines if all third-party content in the scanned file comes from a single source or from multiple sources.

This is done via the orange side bar and orange source match highlighting in the partial matches panel. It represents the union of all source matches across all matched files that are not represented via the currently selected matched file. This allows an auditor to quickly determine whether there are additional source code fingerprint matches in the scanned file that can be explained via an alternate set of matched files.

The yellow bar and highlights represent the Source Code Fingerprint matches found in selected files. The orange bar and highlights represent the Source Code Fingerprint matches found in non-selected files. The combination of the yellow and orange highlights represents the entire set of source code fingerprint matches in the scanned file from all files.



To filter the list of matched files to only those containing the selected text, select a section of text with orange highlights and right-click it and click the **Filter list to Matched Files containing selected text**.

Co		I Matches Tags Groups	arch	Terms					
ihow:	All Matches 🗸 🗸	Contains:		Component	: All Com	ponents .	• X		
Mark	Matched File	Component		Release	CR %	CV %	CL %	υ%	Matc
<b>v</b>	autoglyph.c	opendx 🗸	]	click here to load rele 👻	87.35	100.00	53.77	100.00	159
	glyph.c	opendx 🗸		click here to load rele 💂	87.10	100.00	52.53	100.00	151
	glyph.c	opendx 🗸		click here to load rele 💂	58.58	16.43	4.81	100.00	22
-	glyph.c	opendx 🗸		click here to load rele 💂	58.58	16.43	4.81	100.00	22
	hldhdrs opp	blat _	l i i i	click bere to load rele _	81 84	9.71	100 00	100 00	13
•	Local File:: autoglyph.c								
14 14 15 15 15 15 15 15 15 15 15 15	8 ) 9 else ( 0 if () 2 co 3 ) 4 ) 5 6 7 // jrl 8	<pre>type_string[i] != ' pe_string[count]= t unt++;  begin if ( returnrecei</pre>	.pt t <mark>mp</mark>	_string[i];				W	
16 16 16 16 16	1 2 3 4 5	// Toby Korn // If priorit	tko y i	st to Matched Files contain rn@snl.com 8/4/1999 s specified on the c		ted text		to tl	
16 16 16 16 16	1 2 3 4 5 6	// Toby Korn // If priority if ( priority	tko y i	st to Matched Files contain rn@snl.com 8/4/1999 s specified on the c		ted text		to ti	

### **Displaying Java Name Matches**

Java name space matches are Java classes in the code base that match Names in the signature Compliance Library.

# Task

To display Java name matches, do the following:

- 1. Click the Namespace tab in the lower pane. The Java namespace file tree opens.
- 2. Select a bold filename, and double-click a line item to view the file information.

	Namespace: <u>collections</u>		🔳 🔳 🔲
12 <b>-2 1</b> 2	Name References Depende	encies Declarations	
Entire Workspace	Matched Name ID: N Matched Name: ar	ntr.collections 1470 ntr.collections omponent Listing	
	Name	Title	
	repast	Repast	
ASTPair	vrspace	vrspace	
ByteBuffer	maverick	MaVerickDBMS	
	sds	Software Development Foundation	
	geotools	GeoTools, the java GIS toolkit	
	opennms	OpenNMS	
	jhome	Java Home Automation	
	carbon	Carbon	
	dresden-od	Dresden OCL	
	apg	Another Photo Gallery	
	openuss	FSL - OpenUSS	
LexerSharedInputState     MismatchedTokenException     NoViableAltException     NoViableAltForCharException     ParserSharedInputState     RecognitionException     File Count : 0			

- **3.** Click the **Information** icon for more information about the component. The **Component Info and Attribute** dialog box appears.
- **4.** To assign a version number to the file from the existing list of versions or add a custom version to the list, click the **Plus** button (under the **Component Listing** pane). You can also remove a custom version from components, but you can't remove standard versions because they are predefined entries.
- 5. Click Apply on the Info icon (under the Component Listing pane) to apply your comments and changes.

# **Viewing SCM File Check-In History**

If you configured an SCM application for the current workspace, right-clicking on a file in the file tree allows you to view the that file's recent SCM file check-in history.

Select the View File Check-In History option in the context menu.

# Analyzing Files with Evidence (Third-Party Indicators)

This section explains how the auditor can use Detector for analyzing scan results in files with evidence. Information about analyzing files with evidence is presented in the following sections:

- About Analyzing Files With Evidence
- Researching a File
- Designating Files That Have Been Reviewed
- Tagging Files and Archives
- Filtering Files and Results
- Custom Script-Based Filters

# **About Analyzing Files With Evidence**

The auditor can use Detector for analyzing scan results in files with evidence. The basic auditing work process includes viewing files with a purpose in mind, and then taking action to mark those files that do or do not represent an indication of third-party content in the scanned code base.

The auditing tasks you can accomplish are as follows:

- **Research a file**—When a file contains third-party indicators, you can use the Exact or Partial Matches tab to review the evidence and decide which group best explains the existence of this file. If no such group exists, a new group can be created to explain the file.
- **Customize data**—You can associate a file that appears in the file tree with a product or add a license.
- Annotate (tag) a file—You can add information to a file by tagging the file with any type of data.
- Analyze components and licenses—You can view components and licenses that are part of your project inventory, or research any other components or licenses in the FlexNet Code Insight Compliance Library.
- **Designate which files you have reviewed**—You can mark a file reviewed or unreviewed anytime during the auditing process.

- Filter files—You can filter evidence, much like filtering email. You can sort the files that fulfill certain filter criteria.
- Add a file to a group—Adding files that share characteristics with a group allows you to organize the scanned codebase. It also allows you to give a file a status, in order to slot it appropriately for review during the auditing workflow. Publishing groups results in project inventory.

## **Researching a File**

When a file contains third-party indicators, you can use the Exact or Partial Matches tab to review the evidence and decide which group best explains the existence of this file.

To research (review all evidence) a file, perform the following steps.

### Task To research a file, do the following:

1. Navigate to the file tree.

Ŷ

**Note** • You can filter the tree using evidence tags or a custom filter.)

2. Click on any file in the tree. Files are decorated depending on the types of evidence present in the file. Depending on whether the scanned file is source, archive, or other type of file, the icon preceding it is representative of the file type. The following file notations are available:

Notation	Description
bold	A filename that is in bold contains one or more exact matches.
(!)	A file with a red exclamation mark in front of it contains one or more source matches.
<>	A file with angle brackets in front of it is recognized as a source file based on the file extensions specified in Workspace Settings.           Image: Setting the set of the
Regular weight, no exclamation mark	The absence of bold characters or exclamation marks indicates that the file is neither an exact match nor a source match.
Italics	A file in italics indicates that its status has not yet been received by the server.

Files Namespace	Node: <u>xmlrpc http.h</u>	MD5: 96c8650f7187b22abe65c36c6fc12bde	
	Summary Exact Matches	Partial Matches Tags Groups	
Entire Workspace	Name: Path: Digest: Size:	xmlrpc_http.h C:/Cleanroom/ePortal-1.3/src/blog/xmlrpc_http.h 96c8650f7187b22abe65c36c6fc12bde 2 KB	
	Type: Lines of Code: Last Modified:	Source Code 33 March 17, 2009	
<pre>blog COPYING LICENSE README new.bxt stack.h smlrpc.h mcrypt.c mcrypt.c mcrypt.c mcrypt.c file Count : 83</pre>	Reviewed:	Yes	

**3.** Navigate through the **Evidence** tabs in the file details panel to review the various third- party indicators that were detected in the current file. To view different types of evidence, see Types of Evidence.

# **Designating Files That Have Been Reviewed**

Files in the system can have the following states:

- Not Reviewed
- Reviewed
- Analysis Completed.

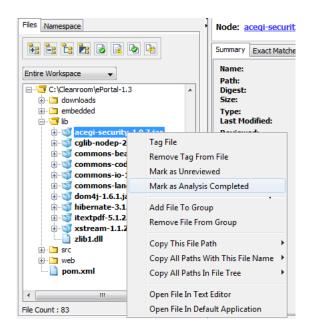
The states of Reviewed and Analysis Completed are related; therefore, only files that are marked as Reviewed can be marked as Analysis Completed and only files that are not marked as Analysis Completed can be unreviewed. A file that has been marked as Reviewed may be brought back to unreviewed state by the scanner during a rescan. See Rescan Options Tab for details. A file that has been marked as *Analysis Completed* cannot be brought out of that state by the scanner. This can only be done by the Auditor using the Detector client.

You can mark a file reviewed, unreviewed, or analysis completed by performing the following steps.



#### To designate a file that has been reviewed, do the following:

- 1. Click on a file in the file tree.
- 2. Right-click to access the commands Reviewed (or unreviewed) and Analysis Complete.



- 3. To designate that an entire directory has been *Reviewed* (or unreviewed) or *Analysis Completed*, select the directory.
- 4. Right-click on the selected directory.
- 5. Select the Mark All Contained Files as Reviewed (or unreviewed) and Analysis Completed.

Files Namespace			: <u>d41d8cd98f00b204e9800998ecf8427e</u>	
Entire Workspace	room\ePortal-1.3	Summary Name: Path: Digest: Size: Type:	lib C:/Cleanroom/ePortal-1.3/lib d41d8cd98f00b204e9800998ecf8427e 4 KB Directory August 5, 2013	
	Add Tag To All Contained Files Remove Tag From All Contained Fi Mark All Contained Files as Review Mark All Contained Files as Unrevie Mark All Contained Files as Analysi Unmark All Contained Files as Anal	ed wed s Complete	August 5, 2013	
	Add All Contained Files To Group Remove All Contained Files From G Copy This Folder Path			
File Count : 83	Copy All Paths In This Folder Copy All Paths In File Tree	•		

# **Tagging Files and Archives**

You can assign tags to files in order to associate arbitrary data to files or to allow custom filtering to be performed using tag values.

• Tagging a File

- Tagging an Entire Directory
- Assigning a Different Value to a Tag

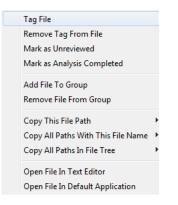
## Tagging a File

To tag a file, perform the following steps.



### To tag a file, do the following, do the following:

- 1. Select the file from the file tree that you wish to tag with one right mouse click.
- 2. Select the Tag File from the Right-Click menu.



The **Add Tag** dialog appears:

Add Tag	X
Tag Name	Owner
Tag Value	Select All
	Add Tag Cancel

- 3. Click the Tag Name you want to apply. It is highlighted.
- 4. Click Add Tag.

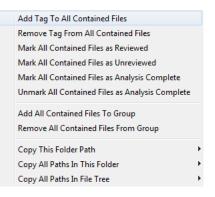
## **Tagging an Entire Directory**

To tag an entire directory, perform the following steps.

# Task

#### To tag an entire directory, do the following:

- 1. Select the directory.
- 2. Right-click to access the command menu that pertains to directories:



3. Select Tag All Contained Files from themenu.

## Assigning a Different Value to a Tag

To assign a different value to a tag, perform the following steps.

# Task

To assign a different value to a tag, do the following:

- 1. Select Tag File from the right-click menu as shown in Assigning a Different Value to a Tag.
- 2. Double-click the Tag Name (in this case, Owner), and the Add Tag dialog appears.

Add Tag	
Tag Name	Owner
	Select All
Tag Value	Fred
	Add Tag Cancel

- **3.** Enter a different value.
- 4. Click OK.

5. Click Add Tag to apply the tag with the new value to the file ordirectory. The tag value appears on the Tag tab of the lower right-hand pane.

Files Namespace	Node: acegi-security-1.0.7.jar MD5: 35	5696bb2e3d3c98925433962	71d4d7 🔳 🔳	
💺 🐂 🐂 🐱 🖬 💊 🐚	Summary Exact Matches Partial Matches Tag	s Groups		
Entire Workspace	Name /	Value	System	
	Contains Exact File Matches	Yes	Yes	
C:\Cleanroom\ePortal-1.3	Contains Indicators	Yes	Yes	
downloads	Owner	Fred	No	
🗈 🛅 embedded	Review Status Last Updated By	alex	Yes	
ė- 🔽 lib	Review Status Last Updated On	08-20-2013	Yes	
acegi-security-1.0.7.jar	Reviewed	Yes	Yes	
cglib-nodep-2.1_3.jar				
⊕-づ commons-beanutils-1.7.0.jar ⊕-づ commons-codec-1.3.jar				
⊕_ S commons-io-1.4.jar				
⊕_j commons-lang-2.3.jar				
⊕_ dom4j-1.6.1.jar				
er i src				
pom.xml				
pom.xm				
۲ III ۲				
File Count : 83		Remove Tag From	n File	

## **Filtering Files and Results**

You can filter evidence, much like filtering email. You can sort the files that fulfill certain filter criteria, and by doing this, you can more easily find files and those components that require the same type of review process. You can also filter results by choosing the last filter you used during your research.

- Filtering Files
- Filter Expression Options

## **Filtering Files**

To filter files based on file information, perform the following steps.



### To filter files, do the following:

- 1. Select the Filter tab in the upper pane, for example.
- 2. Select a line item from the **Filter** pull-down.
- 3. Click the Edit icon at the top of the tab. The Edit Filter page appears.

🍰 Edit Filter		×
Name	ar Files	
Description		
Actions	Add File Path Expression Add Tag Name Expression Add Tag Value Expression	
	File Path X	•
	Path Contains Case Sensitive	
	Value .jar	
	Up Down	_
	Apply Save As Save	

4. Click **Save As** to save the filter settings with a new name, or the **Save** button tosave the filter settings as a future filter choice.

## **Filter Expression Options**

This section contains details related to options you can set during file filtering.

- File Name/Path Expression
- Tag Name Expression
- Tag Value Expression
- Filtering Files by Last Filter Used

### **File Name/Path Expression**

You can use File name expressions to filter files in the scanned codebase tree to include only those matching the criteria of the file name, path, or extension.

There are several operators available for this filter expression, and a case-sensitive comparison can be enabled if required.

### Table 30-1 • Operators

Operator	perator Description	
Contains	Used to find all files that contain a certain String value in the file path	
Does not Contain	Used to find all files that do not contain a certain String value in the file path	
Equals	Used to find all files that exactly match the file path	
Does not Equal	Used to find all files that are do not exactly match the file path	
Starts With	Used to find all files that begin with a certain String value	

### Table 30-1 • Operators

Operator	Description
Ends With	Used to find all files that end with a certain String value (file extension for example)

An example might be all files that contain src in the file path, and end in .java. So the following file would survive such a filter:

\project\modules\core\src\com\mycompany\class\foo.java

### **Tag Name Expression**

Tag name expressions can be used to filter files in the scanned codebase tree to include only those containing a particular tag assignment. This is the expression to use for checking whether a particular system evidence tag is assigned to a given file. An example would show all files with exact file matches that have (or have not) been marked as reviewed.

**Note** • Several tags can be selected. In such a case, the same operator is applied to each tag, and all selected tags must meet the defined criteria for a file to survive the filter.

There are several operators available for this filter expression:

### Table 30-2 • Tag Name Expression Operators

Operator	Description
Has Any Value	Used to find all files that contain any value (including multiple) for the selected tags.
<b>Has Single Value</b> Used to find all files that contain only a single value for the selected tags.	
Has Multiple Values	Used to find all files that contain only multiple values for the selected tags.
Has No Value	Used to find all files that do not contain any values for the selected tags.

🍰 Edit Filter	
Name	Jar Files with Exact File Matches
Description	
Actions	Add File Path Expression         Add Tag Name Expression         Add Tag Value Expression
	File Path X
	Path Contains  Case Sensitive
	Value jar
	Tag Name X
	Available Tags Condition
	Changed Since Last Scan Has Any Value
	Contains Errors
	Contains Exact File Matches
	Contains Indicators Contains License Matches
	Contains License matches
	Contains No Indicators
	Contains Search Term Matches
	Up Down
	Apply Save As Save

### **Tag Value Expression**

Tag value expressions can be used to filter files in the scanned codebase tree to include only those containing a particular value assignment for a specific tag. For example, show all files that contain the string John Smith in the copyright block.

**Note** • Only one tag can be selected for this expression. Also, only files with a given tag assigned will be considered for the comparison. In other words, if Tag A does not have a value for File 1, then File 1 will not be a candidate for surviving a filter value expression for Tag A.

There are several operators available for this filter expression in addition to a **Has Only One Value** option that restricts the comparison to only those files that have a single value assigned for the selected tag:

### Table 30-3 • Tag Value Expression Operators

Operator	Finds
Contains	Files with the selected tag assigned whose value contains the specified string.
Does not Contain	Files with the selected tag assigned whose value does not contain the specified string.

### Table 30-3 • Tag Value Expression Operators

Operator Finds					
Equals	Files with the selected tag assigned whose value is an exact match with the specified string.				
Does not Equal	Files with the selected tag assigned whose value is not an exact match with the specified string.				
Starts With	Files with the selected rag assigned whose value begins with the specified string.				
Ends With	Files with the selected tag assigned whose value ends with the specified string.				

🛃 Edit Filter	
Name	Files with Copyright IBM
Description	
Actions	Add File Path Expression         Add Tag Name Expression         Add Tag Value Expression
	Tag Value X
	Available Tags Condition Contains New Evidence Since Last Revi Contains No Indicators Contains Search Term Matches Contains Version Matches Copyright Holder Detection Evidence Excluded File Disnosition
	Up Down Apply Save As Save

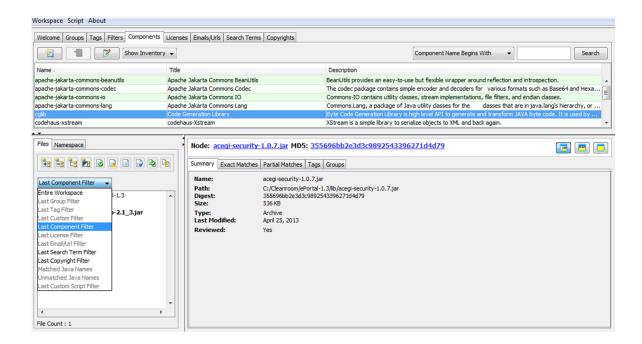
### **Filtering Files by Last Filter Used**

To see the results of the last filter you used to view files in the file tree, perform the following steps.

Task

### To filter files by last filter used, do the following:

- 1. Select a line item, for example, from the **Components** tab.
- 2. Select the last filter type you want to view from the pull-down on the **Files** tab.



## **Custom Script-Based Filters**

There may be cases where complex "custom" logic is required to filter the **Detector** file tree to only the desired files. A custom, Groovy script-based filtering option is available as an add-on to FlexNet Code Insight.

The **Detector Script** menu contains a **Favorite Filters** option that lists all of the Groovy scripts that reside on the client system. The custom filter Groovy scripts should be placed in the following directory:

<USER\_HOME>/.palamida/config/detector/custom\_filters

lcome	Run Script Open Script Console	ense	s Emails/Urls	Search Terms	Copyrights
	Favorite Scripts	•			
	Filter on Top of Existing Tree				
	Favorite Filters	•	Custom-Filt	er-All-Files-By-	Distros.groovy
			Custom-Filt	er-All-Files-By-	Extensions.groovy

Theses Groovy script filters can implement any desired combination of criteria used to filter the list of files in the Detector file tree. The script is passed a list of existing file paths visible in the Detector file tree at the time of execution, and expects a list of file paths returned so that those files can be shown in the Detector file tree.

The **Filter on Top of Existing Tree** option allows the user to control whether the Detector file tree should show all files returned by the custom script filter, or only a subset from the files that are currently visible in the Detector file tree. This option allows sequential filters to be applied to continue filtering the tree until the desired files are remaining.

It is up to the custom script filter to invoke a Filter Options dialog if use-entered options are necessary.

🔊 Filter Options	- • •
Description: This custom filter will reduce the file tree to only those files with the spec Enter a comma-separated list of file extensions below:	ified extensions.
dll,js	
Apply Filter	

After a custom filter is applied, use the **Last Used Filter** pull-down menu to reset the file tree to a previous filtered view. See Filtering Files by Last Filter Used for details.



Chapter 30 Analyzing Files with Evidence (Third-Party Indicators) Custom Script-Based Filters



# **Managing Inventory via Groups**

Information about managing inventory via groups is presented in the following sections:

- About Groups
- Managing Groups
- Creating a Group
- Deleting a Group
- Copying an Existing Group
- Managing Group Details
- Viewing Groups Created by System
- Creating User Groups
- Adding Files to a Group
- Publishing Groups
- Recalling Groups
- Viewing and Confirming Published Inventory

## **About Groups**

Groups are used to organize scanned files. System-generated groups are populated with files that share version, component, or license information. For example, if a set of all files points to one license, it might be assigned a group by the system.

Publishing a group allows those working on the project to see the inventory associated with the project or workspace. As a project owner or auditor, you can create groups or assign files to existing groups. Files in a group can come from multiple workspaces in a project. You can view column headings associated with certain component names that refer to Workspaces as well as Projects.

Policies determine if a component in a group is allowed or disallowed. As an auditor, your job is to look all of the files in a workspace and determine which group best explains the existence (or origin) of that file.

When you publish a group in Detector, in effect, you make it visible as inventory that is ready for review to the entire project team. These project team members can view inventory details including a complete file list associated with the inventory item (published group). You can use the Quick Review feature to immediately review each inventory item, or you can use the complete FlexNet Code Insight workflow to review fully each inventory item using the request form and a formal review process.

The job of the auditor is to fully vet the scanned codebase, and explain the origin of each file by assigning each to appropriate groups. However, once a group is published, it is up to the project team to deal with the review and remediation of the files association with the inventory items (if necessary). Groups that are published from Detector can be viewed by clicking on the Inventory tab in the Project screen.

Recalling a group removes the inventory item from the project. This allows the auditor to do additional analysis on the associated files and re-publish the group or delete it if appropriate.

## **Managing Groups**

Almost all group management can be accomplished from the **Groups** tab of Detector.

ų		Select All	Clear All Publish Rec	al 🔄 Ignored 💟 Empt	y			and a second				Name	•]	Search
0	Name	Priority	Component	License	Owner	System	Updated	Published	Status	F I.	Shi	Workspace Files	Projec	Files
2	codehaus-xstream 1.1.2			BSD 3-clause "New" or "Rev		Yes	08/06/2013	Yes	Ready				1	1
۰.	cglib 2.1	6 - Not Set		Apache License 2.0	System	Yes	08/06/2013	Yes	Ready	. Un Ur	Unk		1	1
	apache-jakarta-commons-lang 2.3		apache-jakarta-commons-lang	Apache License 2.0	System	Yes	08/06/2013	Yes	Ready				1	1
8	apache-jakarta-commons-io 1.4		apache-jakarta-commons-io	Apache License 2.0	System	Yes	08/06/2013	Yes	Ready				1	1
	apache-jakarta-commons-codec 1.3	6 - Not Set	apache-jakarta-commons-codec	Apache License 2.0	System	Yes	08/06/2013	Yes	Ready	. Un Ur	ı Unk		1	1
	apache-jakarta-commons-beanutils 1.7	6 - Not Set	apache-jakarta-commons-beanutils	Apache License 2.0	System	Yes	08/06/2013	Yes	Ready	. Un Ur	ı Unk		1	1
	Files with 'GNU Library General Public Li	6 - Not Set		GNU Library General Public	System	Yes	08/06/2013	No	In Prog	. Un Un	1 Unk		1	1
	Files with 'MIT License' References	6 - Not Set		MIT License	System	Yes	08/06/2013	No	In Prog	. Un Un	Unk		1	1
	opendx	6 - Not Set	opendx	IBM Public License v1.0	alex	No	08/05/2013	Yes	Ready				1	1
	scriptaculous	6 - Not Set	scriptaculous		System	Yes	08/06/2013	Yes	Ready	. Un Un	Unk		5	5
+	: -: -: -: -: -: -: -: -: -: -: -: -: -:		iummary											
Enti	re Workspace 👻		Name: ePortal-1.	-										
_	C:\Cleanroom\ePortal-1.3			oom/ePortal-1.3 8f00b204e9800998ecf8427e										
	downloads		Size: 4KB	6100D204E9800998EC18427E										
			Turner Directory											
	🐵 🛅 embedded		Type: Directory	2013										
			Type: Directory Last Modified: August 5,	2013										

## **Creating a Group**

To create a group, perform the following steps.

# Task

To create a group, do the following:

1. Click the Plus icon (on the top left of the top pane). The Add New Group dialog appears.

- 2. Enter the name for the new group and the owner.
- 3. Click Add New Group to add the group.

## **Deleting a Group**

To delete a group, perform the following steps.



To delete a group, do the following:

- **1.** Select a Group in the table.
- 2. Click the Minus icon. The Group Delete dialog appears.
- 3. Click Yes to delete the group.

# **Copying an Existing Group**

To copy an existing group, perform the following steps.



Task

To copy an existing group, do the following:

- **1.** Select a Group in the table.
- 2. Click the Copy icon. The Copy Group dialog opens.

Copy Group	×
Group Name	Copy of cglib 2.1
Include Files	
Include Metadata	
	OK Cancel

- 3. Configure the copy group options:
  - Include Files—Select to associate files from existing group with the new group.
  - Include Metadata—Select to set group metadata fields for the new group equal to those of the existing group.
- 4. Click **OK** to copy the group.

# **Managing Group Details**

The Group Details tabbed screen provides a tabbed view of various group details. From the General, Notices, and Metadata tabs, you can manage information related to specific group information.

### Table 31-1 • Group Details Screen

Tabs	Description
General	<ul> <li>Group Name, Owner, Title, Description</li> <li>URL</li> <li>Specific criteria for the following values:</li> </ul>
	<ul> <li>Disclosed</li> <li>Status</li> <li>Priority</li> <li>Shipped</li> <li>Modified</li> <li>Remediation</li> <li>Field of Use</li> </ul>
	<ul> <li>Source Distribution Required and URL</li> <li>Components, Versions, Selected Licenses, Possible Licenses, As Found License text, Internal Notes, External Notes, and Detection Notes (read-only)</li> </ul>
Notices	<ul> <li>Include in Third-Party Notices</li> <li>Notice Title, Notice URL, Notice Attribution Statements, Notice Copyright Statements, Notice License URL, Notice License Text, Source Distribution URL, and an option to save current values as a default as well as overriding current values with an available set of default data.</li> </ul>
Metadata	Includes any defined group metadata fields.

Name	mcrypt 2.6.8							G	roup Id: 204	14	
wner	alex Ignored Disclosed									ed 🔄	
itle								P	ublished By	: Alex Rybak (	04/10/2012 17:41)
escription	group desc										
IRL	http://marypt.sourceforge.net/										
	Status	Priority	Shipped	Modified	Remediation	Field of Use					
	Ready for Review 👻	2 - High 👻	Yes 👻	No 👻	No 👻	Core Product		•			
omponent	mcrypt		2	Version	2.6.8		1		]		
elected License	GNU General Public Lice	nse v3.0									
ossible Licenses	Apache License, Version GNU General Public Lice										
As-Found License Text	t /* mcrypt 2.5 - encrypts text or binary files using symmetric algorithms.  For a brief description of the algorithms read the man page. Copyright (C) 1998, 1999, 2000, 2001, 2002, 2007 Nikos Marroy anopoulos  This program is distributed in the hope that it will be useful,  This program is distributed in the hope that it will be useful,										
internal Notes	internal notes										
External Notes	This item is know to pro-	vide encryption of	apability and shou	ld be reviewed f	or export control	compliance.					
Detection Notes			earch terms and vi								

## Managing Third-Party Notices Data for a Group

The use of third-party (TP) and open source software (OSS) is permitted under various open source licenses. In many cases, open source licenses carry with them an obligation that the user of the open source software must provide attribution to the original author. This obligation is generally met by generating a report that includes a list of open source and third-party materials and the licenses under which they are used for the shipping product or application.

FlexNet Code Insight provides a standard third-party notices feature in the product to make this a simple byproduct of the auditing work performed in the product. The following fields comprise a third-party notice for the use of a particular piece of TP/OSS:

Field Name	Field Description
Include in Third-Party Notices	Used to control which audit findings are included in the Third-Party Notices report.
Notice Title	Recommended: Component Version (License) Example: Apache Ant 4.7.1 (Apache License, Version 2.0)
Notice URL	Hyperlink to desired location. Typically, this is to the project homepage.
Notice Attribution Statements	Aggregated list of attribution statements and other notices as-found in the codebase.
Notice Copyright Statements	Aggregated list of "clear" copyright statements as-found in the codebase. May optionally paste in copyright statement from the license text.

### Table 31-2 • Third Party Notices Fields

### Table 31-2 • Third Party Notices Fields

Field Name	Field Description
Notice License URL	Hyperlink to desired location. Typically, this is to the location of the license text.
Notice License Text	The license text as it is to be shown in the Third-Party Notices report.
Source Distribution URL	Location where the source materials are available for a given third- party or open source software item if you are making this available.

The information entered in the third-party notice fields is used to produce an out-of-the-box third-party notices report (from the Web UI).



The principal author and maintainer of mcrypt is

The report contains a block for each item that has been flagged to be included in the report consisting of the following values:

- Notice Title and optional Notice URL.
- An optional Notice Attribution section if the corresponding field has avalue.
- An optional Notice Copyright section if the corresponding field has avalue.

- An optional License Text and URL section if the corresponding fields have values.
- An optional Source Materials URL if the corresponding field has avalue.

Third-party notice fields are located on the Notices tab of the Group Details window in Detector.

A third-party notice can either be defined from scratch for the current group or loaded (using the Load Standard Notice Data button) from the Standard Notices data (if available) and modified as needed. A standard notice applies if the component, version, and license of the notice matches that of the current group. If a standard notice is loaded, it can be modified and saved (using the Save as Standard Notice Data button) as an updated version of the standard notice, or just used for the current group.

General Notices Metadata		
Include in Third-Party Notices	Yes 🔻	
Notice Data	Define My Own   Clear Notices Data Import Notices Data From Group Load Standard Notice Data Save as Standard Notice Data	ata
Notice Title	mcrypt 2.5.8 (GNU General Public License v3.0)	
Notice URL	http://mcrypt.cvs.sourceforge.net/viewvc/mcrypt/	
Notice Attribution Statements		
Notice Copyright Statements	The principal author and maintainer of morypt is	
	Nics Marroyanopoulos <nmax@gnutis.org> Copyright holders in the morypt program are: - Timo Schule <ts@winptchorg> Own all of the OpenPGP related code (rfc2440.c) - Stafan Hetzl <a href="http://whetal@buleneeb.at&gt;">http://whetal@buleneeb.at&gt; Owns the improved werskin of popen() used (popen.c)</a></ts@winptchorg></nmax@gnutis.org>	-
Notike License Text	How to Apply These Terms to Your New Programs If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to male it there activater which everyone can redistribut and change under these terms. To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warrarty; and each file should have at least the Source file and a pointer to where the full induce is found. This program is fere software; you can redistribut and/or mostify R under the terms of the CAN Gerwari Public License as published by the Free Software Foundation, enter version 3 of the License, or (at your option) any later version.	* III *
Source Distribution URL	http://mchypt.cvs.sourceforge.net/	

The Import Notices Data From Group button may be used to copy data from the General Tab to the Notices Detail tab to avoid unnecessary rework if the information has already been entered.

💁 Group Details: (mcrypt 2.6.8)	
General Notices Metadata	
Has Finding Been Reviewed?	Yes
Reviewed By	Lead Auditor
	Save

## Adding or Editing Group Details

To edit or add information to a group, perform the following steps.



To add or edit group details, do the following:

- 1. Select the Group tab.
- 2. Click the **Edit** icon. The Groups Detail tabbed screen appears, allowing you to manage general group information, notes, and notices.

## **Setting Group Status Information**

To set group status information, perform the following steps.

# Task To set group status information, do the following:

- 1. Select the Groups tab in the top pane.
- 2. Click the Edit icon. The Group Details page appears.
- 3. From the Status pull-down, select the correct status for a particular group.

## Managing Licenses for a Group

There are situations where the selected component version for a group has multiple possible licenses— one of which must be selected. An auditor may encounter evidence during an audit that suggests this multiple possible licenses type of scenario, but may not have the ability to make the appropriate selection. In such a case, it is the auditor's responsibility to prepare an accurate list of possible licenses from which a legal user will eventually select the appropriate license from the FlexNet Code Insight web UI during the inventory review process.

For example, a group contains two license fields: Possible Licenses and Selected License. The Possible Licenses field can be edited by the auditor to accurately reflect the list of licenses associated with a given group. The Possible Licenses list is defaulted to the licenses associated with the selected component version if version specific license data is available for the selected component version, or the component itself if version specific license data for the selected component version is not available, or if the version is not selected. The Possible License list can then be edited by the auditor by adding and/or removing any licenses. There is no requirement that the licenses in the Possible License list must be associated with the selected component and/or version. Any changes made to the list of licenses in the Possible Licenses list are for the current group only, and are not reflected in any subsequent groups with the same component and version.

The list of licenses in the Possible Licenses box will define the possible values for the Selected License pull-down. If the auditor knows which license should be selected, then a selection can be made from the Selected License pull-down. This value can then be updated in the FlexNet Code Insight web UI during inventory review.

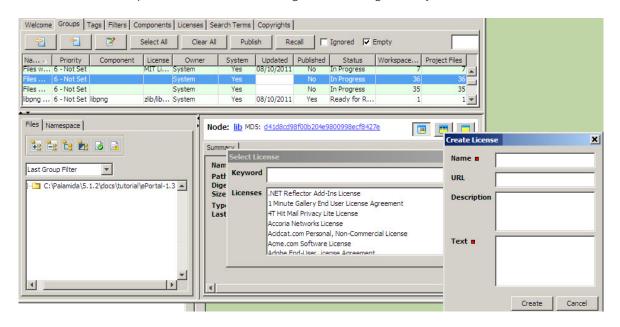
To manage licenses for a group, perform the following steps.

### To manage licenses for a group, do the following:

- 1. Access the Edit Group dialog for the group to which you would like to add license information.
- 2. To add additional possible licenses to the list, click the Plus button under the **Possible Licenses** box. To remove existing licenses from the possible licenses list, select the license to remove, and click the Minus button under the **Possible Licenses** box.

When you click the Plus button, the Select License box appears.

- 3. Select a license from this list or use the Search field to find alicense.
- 4. If you do not see the license that you need, you can create a license by clicking on the Create License button on the **Select License** box.
- 5. The list of licenses in the Possible Licenses box will define the possible values for the Selected License pull-down. If the auditor knows which license should be selected, then a selection can be made from the Selected License pull-down. This value can then be updated in the FlexNet Code Insight web UI during inventory review.



## **Viewing Groups Created by System**

During a scan, the automated analysis detectors create system groups with component, version, and license information pre-selected. To view the system-created groups, perform the following steps.

# Task

Ŷ

Task

### To view system-created groups, do the following:

- 1. Select the **Groups** tab in the top pane.
- 2. Click the **Owner** column, and sort the groups by those created by the system and those created by the users.

## **Creating User Groups**

You may want manually to create groups to organize files representing inventory items or for other purposes such as to organize files to be reviewed by a specific auditor.

To create a user group, perform the following steps.

Task

### To create user groups, do the following:

- 1. Select the **Groups** tab in the top pane.
- 2. Click the Plus icon to add a new group to the list of groups.

Langerter	ata	2 2
ame 🔳	My Group	Group Id: 0
wner	alex	Ignored Disclosed
itle		Published By: None
escription		
RL		
	Status Priority Shipped Modified Remediation Field of Use	
	Not Started <ul> <li>[6 - Not Set •]</li> <li>[Unknown •]</li> <li>[No</li> <li>[No</li> <li>•]</li> </ul>	]
omponent	Version 👘 ·	
elected License	None Selected	-
ossible Licenses		
s-Found License Tex		

The Create Group box opens.

- 3. Enter a name and an owner for the new group. (The owner field defaults to the current userlogin name.)
- 4. Click the Create button.

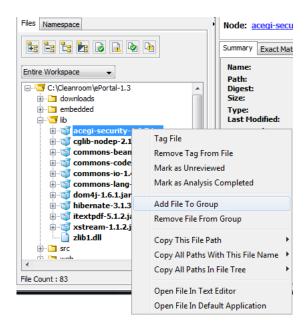
## **Adding Files to a Group**

To add a files to a group, perform the following steps.

# Task

### To add files to a group, do the following:

- **1.** Navigate to the file tree.
- 2. Right-click a single file or a directory (if you want to add all files within that directory).



3. Select Add File to Group. The Add to Group dialog appears:

Add to Group	-	-		-	x
Recent Groups					
My Group					*
Files with 'MIT License (also X11)' References					
apache-jakarta-commons-codec 1.3					
cglib 2.1					
					<b>T</b>
All Groups					
apache-jakarta-commons-beanutils 1.7					
apache-jakarta-commons-codec 1.3					
apache-jakarta-commons-io 1.4					-
apache-jakarta-commons-lang 2.3					E
cglib 2.1					
codehaus-xstream 1.1.2					
dom4j 1.6.1					
Files with 'GNU General Public License v2.0' References					
Files with 'GNU Library General Public License v2.0' References					
Files with 'IBM Public License v1.0' References					
Files with 'MIT License (also X11)' References					
Files with 'MIT License' References					
hibernate 3.1.3					
libpng 1.0.6					
My Group					-
	Ad	ld to Group	reate Group	C	ancel

- 4. Select a group you want to add the file.
- 5. Click Add to Group.

## **Publishing Groups**

To publish groups, perform the following steps.

📋 Task

### To publish groups, do the following:

- 1. On the top pane on the **Groups** tab, select as many groups as you wish to publish by holding down the Control key on the keyboard and left clicking the mousesimultaneously.
- 2. Click Publish to publishonly that group.
- 3. To publish all the groups, click Select All, and then click Publish in the top pane.

# **Recalling Groups**

The following section contains information about different ways to recall groups.

- Recalling a Group from the Individual Group Pane
- Recalling Groups Bulk Fashion

## **Recalling a Group from the Individual Group Pane**

To recall a group is to remove it from the published files, which constitute your inventory. You can recall a group only from the **Groups** tab.

Task

### To recall one group, do the following:

- 1. Select the Groups tab.
- 2. Select the group to recall. To recall a group, the Published column on the **Groups** tab displays **Yes** to indicate that the group is published and part of inventory.
- 3. In the top pane, click **Recall**. The group you selected will be removed from the set of published files and inventory. The **Published** column associated with that group on the **Groups** tab now displays **No**.

## **Recalling Groups Bulk Fashion**

If you need to recall several groups, save time by recalling groups in a bulk fashion.

Task

### To recall groups in a bulk fashion, do the following:

- 1. On the top pane on the **Groups** tab, select as many groups as you wish to recall by holding down the Control key on the keyboard and left clicking the mouse simultaneously.
- 2. Click Recall to recall all of the groups youselected.

3. To recall all of the groups, click **Select All**, and then click **Recall**.

# Viewing and Confirming Published Inventory

After you have published groups, you can confirm that they were published successfully by reviewing the project inventory.

Task	To view and confirm published inventory, do the following:
	1. Click My Projects.

- 2. Click a Project Name link.
- 3. Select the Inventory tab. To search and filter the list, enter terms in the Filter and Search fields.

5umma	ary Workspaces In	ventory	Requests	Tasks	Policies	Comments								
ilter:	All Inventory Items		<b>~</b>	Search:					Q					
d	Name 🔺	Component		L	icense		# Files	30		V	9	Priority	Review Status	Actions
30	oglib 2.1	cglib 2.1		A	pache Softwa	re License, Version 1.1	1	-	-	-	-	3 - Medium	Ready for Review	
29	codehaus-xstream 1.1.2	codehaus-;	xstream 1.1.2	В	ISD License		1	-	-	-	-	3 - Medium	Ready for Review	
84	commons-beanutils 1.7	apache-jak	arta-commons	-beε A	pache License	, Version 2.0	1	-		-	5	3 - Medium	Approved	
33	commons-codec 1.3	apache-jak	arta-commons	-coc A	pache License	, Version 2.0	1	( <b>-</b> )	-	-	-	3 - Medium	Approved	
32	commons-io 1.4	apache-jak	arta-commons	-io1 A	pache License	, Version 2.0	1	-		-	5	3 - Medium	Approved	
31	commons-lang 2.3	apache-jak	arta-commons	alan; A	pache License	, Version 2.0	1	:-::	-	-	-	3 - Medium	Approved	
28	dom4j 1.6.1	dom4j 1.6.1		в	ISD License		1	1		70	5	4 - Low	Approved	
27	hibernate 3.1.3	hibernate 3	.1.3	G	NU Lesser Gei	neral Public License (LG	1	()	-	-	-	3 - Medium	Ready for Review	
26	libpng 1.0.6	libpng 1.0.6		N	lone Selected		1	0	-	20	5	3 - Medium	Ready for Review	
25	mysql-connector-j 5.0.5	mysql-conn	nector-j 5.0.5	G	NU General Pu	blic License (GPL), Ver	1	-	-	-	-	3 - Medium	Rejected	

Chapter 31 Managing Inventory via Groups Viewing and Confirming Published Inventory



# **Working with Archives**

If your codebase contains supported archive types and was scanned with the "Scan Files Inside Archives" option enabled in Workspace Settings, you will be able to view different evidence types and operate on both the archive's outer file (such as foo.jar) as well as for the archive's inner files (all files located inside foo.jar) in Detector. For information on how to configure your workspace to scan files inside archives, see Detection Tab Tasks.

- Supported Archive Types
- Types of Evidence
- Viewing Evidence
- Groups
- Tags
- Archive File Counts/Nested Archives
- Tagging an Archive for Scanning
- Archive File Operations

## **Supported Archive Types**

Cab, ear, jar, rpm, sar, tar, tar.bz, tar.bz2, tar.bzip2, tbz, tgz, war and zip are supported archive types. For an up-to-date list of supported types, go to **Workspace Settings > Detection Tab > Archive Scanning Options** at the bottom of the page.

## **Types of Evidence**

The following are the types of third-party indicators available as part of the scan results for archives and their contents:

- Exact Matches, Copyrights
- Emails and/or URLs
- Search Term matches

License matches

Automated Analysis techniques such as Auto-WriteUp, POM File Analyzer and MID Rule Detection are also available for archives and are reflected in the scan results. See Automated Analysis Tab for information on how to enable these techniques.

### **Source Matches**

Files inside archives are not scanned and tagged for Source matches. For extended analysis on files inside archives, it is recommended that you manually unpack the archive before performing a scan.

### **Exact Matches**

There are two types of archives: those with exact matches and those without exact matches.

### **Archives with Exact Matches**

During a FlexNet Code Insight scan, archives that are found to contain an Exact match (digest match) on the outer file are tagged with the "Contains Exact File Matches" tag, while inner files of these archives are not tagged for Exact matches and therefore will not display the tag. This behavior is in place as a performance enhancement and is reflected in the group/tag file counts. These files are still analyzed and tagged for all other evidence types, including Copyrights, Emails and/or URLs, Search Term matches and License matches. The "Contains Indicators" tag is applied to inner files of archives with Exact matches only if one of these four evidence types is detected and is not applied otherwise.

For example, if a scan reveals that foo.jar has an Exact match to a component in the FlexNet Code Insight CL, it will be tagged with the "Contains Exact File Matches" tag. Its inner files however, such as foo.jar/License.txt, will not display this tag but may display other tags such as the "Contains License Matches" and "Contains Indicators."

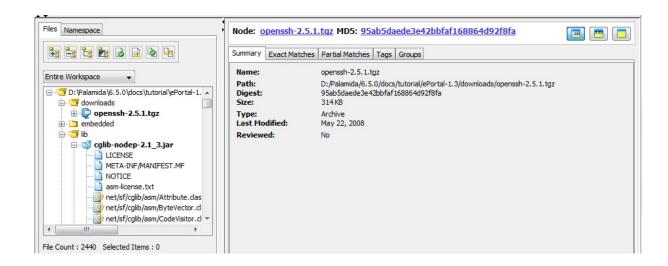
### **Archives without Exact Matches**

Archives that do not contain an Exact match (digest match) on the outer file are further analyzed for Exact matches on the inner files. If an inner file is found to contain an Exact match, it will be tagged with the "Contains Exact File Matches" tag and the "Contains Indicators" tag.

For example, if a scan reveals that foo.jar does not have an Exact match to a component in the FlexNet Code Insight CL, its inner files will be further analyzed for Exact matches. If foo.jar/License.txt is then identified as an Exact match to a component in the FlexNet Code Insight CL, it will be tagged with the "Contains Exact File Matches" tag and the "Contains Indicators" tag, as well as any other tags reflecting the detected evidence.

## **Viewing Evidence**

To access the contents of an archive press the (+) icon to the left of the archive name in the file tree located in the Files tab. This will expand the archive, allowing you to view evidence for and operate on the files inside the archive.



## Groups

You can view the groups that an archive file belongs to by selecting the file in the file tree and switching to the Groups tab in the lower pane.

If a file inside an archive triggers an automated detection technique such as Multi-Indicator Detector (MID Rule) or Auto-WriteUp, the file will be added to the appropriate System Group. Alternatively, inner files of archives, the archive outer file, or both types of files can be manually added to a group.



**Note** • Adding an inner file of an archive to a group will not automatically add the archive outer file to the group and adding an archive outer file to a group will not automatically add the archive's inner files to the group. Group file counts in the "Workspace Files" and "Workspace Unreviewed Files" column reflect this behavior and may be smaller than the File Count in the file tree.

For more information on groups, see Managing Groups.

										Name		•	Search
Name 2	Description			Туре	Syste	m	Wor	kspace Fil	es		Workspace L	nreviewed	Files
ontains Errors	File Has Scan	Error		Pick List		Yes					0		0
ontains Exact File Matches	File Contains	Exact Match	hes to Other Fil	es Pick List		Yes				47	3		473
ontains Indicators	File Contains	Third-Party	Indicators	Pick List		Yes				51	8		518
ontains License Matches	File Contains	License Mat	tches	Pick List		Yes				3	0		30
ontains No Indicators	File Contains	No Third-Pa	arty Indicators	Pick List		Yes				192	2		1922
ontains Search Term Matches	File Contains	Search Terr	m Matches	Pick List		Yes					0		0
ontains Source Matches	File Contains	Source Cod	le Fingerprint M	atches Pick List		Yes					8		8
opyright Holder	Copyright Ho	lder		Free Text		Yes				17	5		175
A REAL PROPERTY OF THE REAL PR	and the second second second			the second second		Yes				-	20		
	Matched by A			c MD5: <u>b2efe3e2</u> a	30735b3	M==	a1048ct	0440c			1		51
iles Namespace		Node: s	sh/auth-rsa.	<u>c MD5: b2efe3e2a</u>	_	352d3e	a1048ct	0 <u>440c</u>					^
iles Namespace		Node: ss	sh/auth-rsa. Exact Matches	Postation	gs Groups	352d3e			Publi				^ []
etection Evidence		Node: ss	sh/auth-rsa. Exact Matches Name Pri	c MD5: b2efe3e2a	gs Groups	352d3e Owner	System			Status		. Shi	- P

# Tags

You can view tags for an archive file by selecting the file in the file tree and switching to the Tags tab in the lower pane.

				Name	•	Search
Name /	Description	Туре	System	Workspace Files	Workspace Unreviewed	Files
Analysis Completed	Analysis Completed for This File	Pick List	Yes		0	0
Changed Since Last Scan	File Has Changed Since Last Scan	Pick List	Yes		0	0
Changed Since Workspace Copy	File Changed Since Workspace Copy	Pick List	Yes		0	0
Contains Email/URL Matches	File Contains Email or URL Matches	Pick List	Yes	14	4	144
Contains Errors	File Has Scan Error	Pick List	Yes		0	0
Contains Exact File Matches	File Contains Exact Matches to Other Files	Pick List	Yes	47	3	473
Contains Indicators	File Contains Third-Party Indicators	Pick List	Yes	51	8	518
Contains License Matches	File Contains License Matches	Pick List	Yes	3	0	30
Contains No Indicators	File Contains No Third-Party Indicators	Pick List	Yes	192	2	1922
Contains Counds Town Matches	Cile Containe Counds Town Matchine	Diels Link	V		0	0

Summary Exact Matches	Partial Matches Tags Groups		
Name /	Value	System	
Contains Email/URL Matches	Yes	Yes	
net/sf/cglib/util/Parallel5  Contains Indicators	Yes	Yes	
net/sf/cglib/util/ParallelS Contains License Matches	Yes	Yes	
net/sf/cglib/util/ParallelS Copyright Holder	-unparseable-	Yes	
/sf/cglib/util/SorterTe In Group	Yes	Yes	
META-INF MANTEST.MF MANTEST.MF NOTICE.txt g org 			

If a file inside an archive contains third-party indicators such as Exact Matches, the appropriate system tags will be applied to the file. Alternatively, you can manually add a tag to inner files of archives, the archive outer file, or both types of files.

_	0	
-	_	
_	_	

**Note** • Adding a tag to inner files of an archive will not automatically add the tag to the archive outer file and adding a tag to the archive outer file will not automatically add the tag to the archive's inner files. Tag file counts in the "Workspace Files" and "Workspace Unreviewed Files" columns reflect this behavior and may be significantly smaller than the File Count in the file tree.

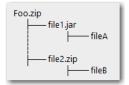
For more information on tags, refer to Tagging Files and Archives.

# **Archive File Counts/Nested Archives**

The File Count located at the bottom left-hand corner of the Detector file tree represents the total number of files currently in the file tree. In the presence of nested archives (archives that contain multiple levels of sub-archives) the File Count for an archive in the tree will always consist of the outer-most archive file + each file inside the archive.

Name > nalysis Completed hanged Since Last Scan hanged Since Workspace Copy ontains Email/URL Matches ontains Errors	Description Analysis Completed for This File File Has Changed Since Last Scan	Type Pick List	System	Workspace Files	Workspace Unreviewed Files
hanged Since Last Scan hanged Since Workspace Copy ontains Email/URL Matches ontains Errors	File Has Changed Since Last Scan	There was a			
hanged Since Workspace Copy ontains Email/URL Matches ontains Errors	2		Yes	0	
ontains Email/URL Matches ontains Errors		Pick List	Yes	0	
ontains Errors	File Changed Since Workspace Copy	Pick List	Yes	0	1
	File Contains Email or URL Matches	Pick List	Yes	144	14
	File Has Scan Error	Pick List	Yes	0	
ontains Exact File Matches	File Contains Exact Matches to Other Files	Pick List	Yes	29	2
ontains Indicators	File Contains Third-Party Indicators	Pick List	Yes	218	21
ontains License Matches	File Contains License Matches	Pick List	Yes	30	3
ontains No Indicators	File Contains No Third-Party Indicators	Pick List	Yes	35	3
	Summary				
Entire Workspace	\ePortal-1.				

For example, the file count for foo.zip in the following tree structure, will equal 3. Only Foo.zip, fileA and fileB are included in the count while file1.jar and file2.zip are treated as directories and are not included in the count.



**Note** • The file counts in the "Workspace Files" and "Workspace Unreviewed Files" columns in the Groups and the Tags tabs may be significantly smaller than the File Count in the file tree. This is due to the fact that group/tag file counts do not always represent inner files of archives, while the File Count in the file tree always includes inner files of archives.

# **Tagging an Archive for Scanning**

The Tag Archive for Scanning operation can be used to tag a specific archive for future scanning. This is useful if for example you did not originally select the Scan Files Inside Archives option in Workspace Settings and want to scan one or more select archive files in your codebase. To tag an archive for future scanning, right-click the archive in the file tree and use the "Tag Archive for Scanning" option from the right-click menu. If you wish to tag all contained archives inside an archive or in a directory, use the "Tag All Contained Archives for Scanning" option instead.

## **Archive File Operations**

Scanned archives are treated both as self-contained nodes (individual files) as well as directories that contain files and therefore both single-file operations as well as directory operations are available for archives in the right-click menu.

Welcome Groups Tags Filters Comp	onents Licenses Emails/Urls Search Ter	ms Copyrights			
				Name	▼ Search
Name >	Description	Туре	System	Workspace Files	Workspace Unreviewed Files
Analysis Completed	Analysis Completed for This File	Pick List	Yes	0	0
Changed Since Last Scan	File Has Changed Since Last Scan	Pick List	Yes	0	0
Changed Since Workspace Copy	File Changed Since Workspace Copy	Pick List	Yes	0	0
Contains Email/URL Matches	File Contains Email or URL Matches	Pick List	Yes	144	144
Contains Errors	File Has Scan Error	Pick List	Yes	0	0
Contains Exact File Matches	File Contains Exact Matches to Other Files	Pick List	Yes	29	29
Contains Indicators	File Contains Third-Party Indicators	Pick List	Yes	218	218
Contains License Matches	File Contains License Matches	Pick List	Yes	30	30
Contains No Indicators	File Contains No Third-Party Indicators	Pick List	Yes	35	35
Cambring Canada Tanna Madalana	Tile Containe Connels Town Matches	Dieletteek	M	0	
Entire Workspace					
File Count : 2440 Selected Items : 0	• •				

Applying any of the following single-file operations affects only the archive (outer file) without affecting the inner files:

- Tag File
- Remove Tag From File
- Mark as Reviewed
- Mark as Analysis Completed

- Tag Archive for Scanning
- Add File to Group
- Remove File from Group

## **Directory Operations for Archives**

Applying the following directory operations affects only the files inside the archive without affecting the archive (outer file):

- Add Tag To All Contained Files
- Remove Tag From All Contained Files
- Mark All Contained Files as Reviewed
- Mark All Contained Files as Unreviewed
- Mark All Contained Files as Analysis Complete
- Unmark All Contained Files As Analysis Complete
- Tag All Contained Archives for Scanning
- Untag All Contained Archives for Scanning
- Add All Contained Files To Group
- Remove All Contained Files From Group

## **Bulk-File Operations for Archives**

To select all the files inside the archive, select the archive (outer file), press and hold down the Shift key, and press the left mouse button.

Chapter 32 Working with Archives

Archive File Operations



# **Using Multi-Select for Bulk Operations**

This section contains the following topic:

• Selecting and Clearing with Multi-Select

# Selecting and Clearing with Multi-Select

To apply a file operation to several files or folders, use the multi-select feature to make the selection.

There are several ways to select multiple files or folders, as described in the following sections.

### Consecutive

To select any consecutive group of files or folders, left-click the first item, press and hold down the Shift key, and left-click the last item.

### **Non-Consecutive**

To select non-consecutive files or folders, press and hold down the Ctrl key, and left-click each item that you want to select.

### **Files Inside Archives**

To select all the files inside the archive, select the archive (outer file), press and hold down the Shift key, and then press the left mouse button.

### **Clear Selection**

To clear a selection, click the selection again with the left-mouse button.

Chapter 33 Using Multi-Select for Bulk Operations

Selecting and Clearing with Multi-Select



# **Detector Code Search**

This section contains the following topics:

- Detector
- Code Search Examples
- Special Characters
- Using Code Search for Binary Files
- Customizing Code Search Indexing
- Detector Code Search APIs

## **Detector**

Detector Code Search provides the ability to quickly search across the scanned codebase for search terms, strings, file names, file paths or any combination. In addition to those capabilities, Detector Code Search provides the following:

- Multiple ways to invoke search.
- Search history per session
- Support for binary files
- Ability to add file types for indexing
- Ability to specify exclusions

## **Code Search Indexing**

Code Search indexing is enabled on all workspaces by default. When the workspace is scanned for the first time, an index is created and placed into the <workspaceDirectory>/<projectName>/index/ directory of your FlexNet Code Insight installation. If the workspace is rescanned, the data is re-indexed, ensuring that the index is always up-to-date.

## **Disabling Code Search Indexing**

Follow these instructions to disable Code Search indexing.

# Task

### To disable Code Search indexing, do the following:

- 1. Open scan.properties, located in <FNCI\_Root\_Dir>/config/scanEngine/.
- 2. Add the following property and set it to *false*:

workspaceIndexing = false

3. Restart the server.

## Launching Code Search

You can launch Code Search in any of the following ways:

- By using the Code Search icon above the file tree.
- From the Partial Matches panel.
- From the file tree itself.

## Using the Code Search Icon

Use the search icon above the file tree to open the **Search Codebase** dialog, which offers full search functionality, including the ability to select a context and view recent search history. The search supports simple or complex queries with wildcards and conjunction operators. See examples for constructing the search query in Code Search Examples.



To launch Code Search with the icon, do the following:

1. Select the search icon (), which appears above the file tree. The **Search Codebase** dialog appears:

Workspace Script Options About Wekome Groups Tags Filters Components I	Search Codebase Search file contents or see <u>Examples</u> fname:stack.h "Herman Bloggs" Search Clear Context: @ Entire File Tree  Filt		Empt	у				
ID / Name Priority Component Li	Recent Searches for Current Session	1		Field of	Include	Shipp	Workspa	Pr
227 zlib 1 6 - Not Set zlib zli	Search Query	Search Res	ess		Unknown		3	3
228 zlib 1 6 - Not Set zlib zli		Search Kes	ess	ornoronni	Unknown	ornanorm	1	L
229 zlib 1 6 - Not Set zlib zli	fname:stack.h "Herman Bloggs"	1	ess		Unknown		1	L
230 zlib 1 6 - Not Set zlib zli	General Public License	6	ess		Unknown		1	L
234 protot 6 - Not Set prototype MI	copyright	16	ess		Unknown		1	L
235 libpng 6 - Not Set libpng zli	stolen from	0	ess		Unknown		1	L
237 libjpeg 6 - Not Set libjpeg In	time	5	ess		Unknown		1	L
255 Files 6 - Not Set MI	time MIT	0	ess		Unknown		7	1
256 Files 6 - Not Set IB	GPL	4	ess	Unknown	Unknown	Unkno	1	L
Files Namespace	Summary Exact Matches Partial Mat Copyrights Email/URLs Local File:: stack.h 1 /* 2 * gaim - Blogger (xml-rp 3 * 4 * Copyright (C) 2003, File	ense Matches Search				Code Se	arch Findings	

2. Type your query in the search field. For examples of search queries, see Code Search Examples.

## Using the File Context Menu: File Name Search

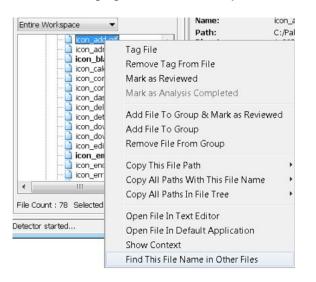
A search for a file name contained in the codebase can be quickly executed by highlighting the file in the file tree, and selecting the option to Find This File Name in Other Files from the context menu. This is useful for finding references to files with an unknown origin in the code.



### Task

### To use the File Name Search, do the following:

1. In the file tree, highlight the name of the file you want to search for in your codebase. The context menu opens:



2. Select Find This File Name in Other Files from the context menu. Detector searches your codebase for the filename you selected.

Note . This type of search always applies to the	urrent contaxt (filtar

**Note** • This type of search always applies to the current context (filtered file tree).

### **Using the Partial Matches Panel String Search**

You can search directly from the **Partial Matches** panel. If you come across an interesting string, highlight it and select the **Find selected text in other files** option from the context menu to filter the file tree to only those files that contain the selected string.



Task

To use the Partial Matches Panel String search, do the following:

1. Select a file from the file tree and navigate to the **Partial Matches** tab.

2. Highlight a portion of the text that is of interest and select **Find selected text in other files** from the context menu:

Files Namespace	Node:         autoglyph.c         MD5:         f66b4d0a08608db1be221604cb781d17
H: H: H: D R 🖉 🕒 😫	Summary Exact Matches Partial Matches Tags Groups
Last Tag Filter 💌	Copyrights Email/URLs License Matches Search Terms Source Matches Lucene Findings File T
C:\Palamida\6.8\docs\tutorial\ePor	Local File:: autoglyph.c Whet me Dimensional Decision typedef struct Disconne float x; float x; float x; Point2D; bypedef struct arg ( 0bject outobject;

The file tree is filtered to show only those files that contain the selected string.

# **Code Search Examples**

The following table lists code search examples.

### Table 34-1 • Code Search Examples

Туре	Search	Finds Files
Search terms	do it right	Containing terms "do", "it" and "right" anywhere in the file contents. The default conjunction operator is <i>AND</i> if no operator is specified.
Search phrase	"do it right"	Containing phrase "do it right" in the file contents.
	"jonny@flexera.com"	Containing email phrase "jonny@flexera.com" in the file contents.
file name	fname:stack.h	That are named "stack.h".
file path	<pre>fpath:/home/palamida/ePortal- 1.3/* [Linux] fpath:c:/palamida/ePortal-1.3/* [Windows]</pre>	That are located in the ePortal-1.3 directory or below.
?	te?t	Containing "test" or "text" in the file contents.
*	test*	Containing "test", "testing" or "tested" in the file contents.
AND	"jakarta apache" AND "Apache Lucene"	Containing both "jakarta apache" and "Apache Lucene" in the file contents.
OR	"jakarta apache" OR "Apache Lucene"	Containing either "jakarta apache" or "Apache Lucene" in the file contents.

#### Table 34-1 • Code Search Examples

Туре	Search	Finds Files
NOT	"zlib compression library" NOT "zlibc Compressing File-I/O Library"?	Containing "zlib compression library" but not "zlibc Compressing File-I/O Library" in the file contents.
grouping	("Log4j" OR "Log4j 2") AND website	Containing "Log4j", "Log4j 2", or both in addition to "website" in the file contents.
compounding	<pre>fname:stack.h ("GPL" OR "General Public")</pre>	That are named "stack.h" and have "GPL" or "General Public" in the file contents.

#### Additional Information

- The default conjunction operator is AND. If is no operator is specified between two terms, the AND operator applies.
- Searches are not case sensitive (including conjunction operators).
- You may use an asterisk (\*) as the first character of a search.
- See Lucene Query Parser Syntax for advanced options.

### **Special Characters**

A list of special characters and their interpretation is provided below. If you prefer these characters to be interpreted as search data, the characters must be escaped by placing a backslash (\) character immediately before. Within a phrase, characters are interpreted as search data and need not be escaped. A phrase is one or more terms surrounded by quotation marks.

#### Table 34-2 • Special Characters

Special Characters	Description
* 0-n	n char wildcard
?	One-character wildcard
:	Follows field name
"	Begins or ends phrase
~	Similar or proximity search
!	Same as NOT
&&	Same as AND
I	Same as OR
()	Groups terms

#### Table 34-2 • Special Characters

Special Characters	Description
{}	Exclusive range
[]	Inclusive range
1	Escapes next char
+	Preceding must have term
-	Preceding must not have term
٨	Boosts term

## **Using Code Search for Binary Files**

Code Search uses two different mechanisms for processing binary files. The mechanism used determines whether highlights are available in Detector for the search results.

- Highlighting is supported for file types specified by the indexBinList property. By default, these include *dll, exe, jar, rpm* file types.
- Highlighting is not supported for all other binary file types (not specified by the indexBinList property) such as *doc*, *docx* and *ppt* file types. If working with these types of files, you can use the CTRL-F command to locate specific search terms within the file.

## **Customizing Code Search Indexing**

The following properties may be added to the scan.properties file to further customize indexing and processing of binary files during indexing.

Important • Restart the server if you add or modify any of these properties.

Table 34-3 • Code Search Binary Support Properties

Property	Details
workspaceIndexing = true	Set to <i>true</i> to enable indexing for the next scan. Set to <i>false</i> to turn it off. <i>Default</i> = <i>true</i>
indexExcludeList =	Comma separated list of file extensions to append to the internal predefined set of extensions (see <b>Workspace Settings &gt; General &gt; Excluded File Patterns</b> for existing list) that will be excluded from Code Search indexing.

#### Table 34-3 • Code Search Binary Support Properties

Property	Details
indexSrcList =	Comma separated list of file extensions to append to the internal predefined set of extensions (see <b>Workspace Settings &gt; Languages – Extensions</b> for existing list) that will be processed and indexed by Code Search. <i>Default = empty</i>
indexBinList = dll, exe, jar, rpm	Comma separated list of extensions to process as binary data <i>(index without Tika using US-ASCII to minimize junk terms)</i> . Highlights are available. Default = dll, exe, jar, rpm
indexTikaParseLen = 10485760	Limits the number of characters per file processed by Apache Tika. Use -1 to process the entire file and 0 to not process any file using Tika. indexTikaParseLen = n implies Tika will process up to n characters per file. Default = 10485760

**Note** • All binary files not specified by the indexBinList property are processed by Apache Tika. Apache Tika typically generates a much larger index and can take a long time to run. In the case that you experience a system hang during indexing, it is recommended that you set "indexTikaParseLen = 0" to limit the number of characters processed by Tika.

### **Detector Code Search APIs**

Limited API support is available for Code Search. A ScriptRunner script may be used to invoke a REST API to search one or more indexes. There are methods to do the following:

- Search an index
- Search one or more indexes
- Test if an index exists

Visit the Customer Community at https://flexeracommunity.force.com/customer/ContactSupport for additional information on these APIs and a sample script.

Chapter 34 Detector Code Search

Detector Code Search APIs



## **Generating Custom Fingerprints**

This section contains the following topics:

- Custom Fingerprints
- customFingerprints.groovy Options

## **Custom Fingerprints**

Custom data, including custom source code fingerprints and custom digests, are managed centrally in the application. This means that custom fingerprints and digests will be picked up by all workspaces. If you need to isolate custom data to a particular workspace, contact Flexera SCA Support from the Customer Community page https://flexeracommunity.force.com/customer/CCContactSupport.

Custom fingerprint generation is controlled by an XML configuration file. The template for this file is located in:

scriptRunner/scripts/customFingerprints\_template.xml

All custom data is centralized, so you must always modify this file when generating custom fingerprints. The basic instructions for generating custom fingerprints are as follows:.



#### To generate custom fingerprints, do the following:

- 1. Go to the scriptRunner/scripts directory and make a copy of the customFingerprints\_template.xml file. You can edit this file or make a copy of it. For example purposes, we assume we are editing the customFingerprints\_template.xml file in these instructions.
- 2. Edit the customFingerprints\_template.xml file located in the scriptRunner/scripts directory as follows, and save the file when finished:

Line	Code
<b>Line 14:</b> Set the output directory to point to the corporate workspaces directory:.	outputDir="Palamida/workspaces/CorporateWS">

Line	Code
<b>Line 22:</b> Set the product name for which you are generating SCF.	<product name="component_foo"></product>
<b>Line 23:</b> Set the release name for every distinct release for which you are generating SCF.	<release name="component_foo_1.0.zip"> <release name="component_foo_1.2.zip"></release></release>
<b>Line 28:</b> Provide a directory where the source code for the fingerprints is located.	<fileset dir="/Palamida/custom/foo_directory"> Note • You must provide the path to the directory, not the file path. Custom SCFs will be generated for all the files under this directory.</fileset>

- 3. Ensure the FlexNet Code Insight Server is running.
- 4. Invoke scriptRunner to generate custom fingerprints:

```
<CODE_INSIGHT_ROOT_DIR>/6.13.x/scriptRunner/bin/./scriptRunner.sh customFingerprints.groovy -d customFingerprints_template.xml
```

or (if you are on Windows)

```
<CODE_INSIGHT_ROOT_DIR>/6.13.x/scriptRunner/bin/scriptRunner.bat customFingerprints.groovy
    -d customFingerprints_template.xml
```

5. Wait for the script to finish, which can take a long time if you are processing a large number of files.



Note • It is no longer necessary to publish the CorporateWS with a script as it was in previous versions of the product.

**6.** Rescan any compliance workspaces that you want to pick up the new custom fingerprints. New workspaces will automatically pick up the custom fingerprints.

## customFingerprints.groovy Options

The following options can provide you more detailed match information:

Table 35-1 • Additional Options for customFingerprints.groovy

Option	Description
-d	This option applied to the fingerprint compiler causes a digest record to be created for every file that is processed. If you do not specify the <b>-d</b> option, you will not get digest matches on exact copies of the files processed by the fingerprint compiler.
-a	This option generates fingerprints for files inside archives. Otherwise, the fingerprint compiler will not go inside archive files.
-v	This option gives you more detailed information in the scriptRunner/log/scriptRunner.log.



# **Upload to Scan**

Upload to Scan allows the project Owner or auditor of a project to upload content to a designated scan server and (optionally) automatically invoke a scan/report on the uploaded content. Upload to Scan can be run as an upload only or as an upload immediately followed by a scan/report.

- Configuring Upload to Scan
- Prerequisites
- Using Upload to Scan

## **Configuring Upload to Scan**

As a security precaution, Upload to Scan must be activated and configured by a system administrator in core.properties and scanEngine.properties before it is available for use.



#### To configure Upload to Scan, do the following:

- 1. Stop Tomcat. You can use shutdown.bat from the \bin directory or a similar command.
- 2. Configure the following properties:
  - core.properties
  - scanEngine.properties
- 3. Restart Tomcat to make the Upload to Scan feature available in the Web UI.



Note • Upload to Scan will not work if any of these properties are missing. Sample values are provided below.

### core.properties

Configure the core.properties property as described below.

#### Table 36-1 • core.properties

Property	Description	
<pre>Set to "true" to enable upload upload.to.scan.enable.core = true</pre>	Enables upload functionality (without scanning) on the Core server from the Upload to Scan page. Required for Upload to Scan to work.	
	<b>Note</b> • Files are uploaded, never unpacked on the Core server.	
<pre>Max upload file size in MB upload.to.scan.max.file.size = 10240  Note • Must be an integer.</pre>	Indicates the maximum supported file size for upload. Defaults to 10 GB. Files above max file size will not be uploaded.	
Reports to be available on the Upload to Scan page (quoted, comma-delimited list) upload.to.scan.reports.list = "Scanned Files Report", "Third-Party Indicators Report", "Palamida Analyzer - Quick Assessment, "Palamida Analyzer - Group Builder"	Indicates the set of reports that should show up on the Upload to Scan page. Leave blank if you do not want any reports to be available to the user during Upload to Scan.	
<ul> <li>Set upload.to.scan.do.scan to "true" or "false":</li> <li>True—Allow upload followed by a scan/report task (Upload and Scan).</li> <li>False—Allow upload only (Upload).</li> <li>upload.to.scan.do.scan = true</li> </ul>	Enables the scan functionality from the Upload to Scan page. If set to false, only upload is available without the option to scan.	
Alias of the scan server to which files will be uploaded upload.to.scan.scanner.alias = Scanner1	Indicates the scan server to which files are uploaded from Upload to Scan. Specify multiple scanners with a comma-delimited list (such as Scanner1, Scanner2, Scanner3).	

### scanEngine.properties

Configure the scanEngine.properties property as described below

#### Table 36-2 • scanEngine.properties

Property	Description	
Set uploadToScanEnableScanner to "true" to enable Upload to Scan	Enables upload functionality on the scan server where this property file resides. Required for Upload to Scan to work.	
uploadToScanEnableScanner = true		
<b>Upload directory to write to</b> uploadToScanUploadDirectory = /home/	Indicates the directory on the scan server where files will be uploaded during Upload to Scan.	
upload_to_scan_folder	Required for Upload to Scan functionality.	
	<b></b>	
	<i>Important</i> • Must be an absolute path, equal to or a child of the serverFileSystemRoot directory.	
Web application uses this property to limit the root of server file system	Indicates the root directory on the scan server where files will be scanned. Users may not browse and scan directories	
Multiple roots are supported, but they have to be separated by " ". For example, in Windows:	outside of this root. Required for Upload to Scan functionality.	
C:\\Windows C:\\Folder1\\Folder2 D:\\Folder3		
serverFileSystemRoot	Important • Must be equal to, or a parent of the upLoadToScanUpLoadDirectory.	

## Prerequisites

Upload to Scan has the following prerequisites.

- Supported File Types
- File Permissions
- Upload Size
- Using Upload to Scan
- Limitations
- Error Handling
- Security Features

### **Supported File Types**

Upload to Scan supports the following file types:

- Single file upload: supported for all file types.
- Multiple files: may be uploaded in archived form (S, rpm, tgz, or tar.gz). If the system detects one of these file types, the file is expanded on the scan server and the compressed file and any temporary files are discarded. The contents of the archive are then scanned. If the extracted file contents include other compressed files, these files remain compressed. All other types of archives (e.g., exe or jar) are treated as single files.

### **File Permissions**

All uploaded files have their permissions changed to "read only" and "non-executable". All directories have their permissions changed to "read only" and "executable".

On Linux systems, directories must be "executable" to be read.

### **Upload Size**

The default maximum upload file size is 10240 MB or approximately 10 GB.

The upload.to.scan.max.file.size property in core.properties may be used to change the maximum upload size.

## **Using Upload to Scan**

To use Upload to Scan, perform the following steps.

## Task

To use Upload to Scan, do the following:

- 1. Log into FlexNet Code Insight as an *auditor* or *project owner*.
- 2. Navigate to My Project Details for the project you want to upload and scan.
- 3. Select the Summary tab:

💋 My Project			
Summary Workspaces	Inventory Requests Tasks Policies Comments Attachments		
Id	4		
Name	My Project		
Team	team1		
Owner	Project Owner		
Auditors	There have been no Auditors selected for this project.		
Security Analysts	There have been no Security Analysts selected for this project.		
Observers	There have been no Observers selected for this project.		
QuickReview Facilitators	admin admin		
Advanced Options	Enable Inventory Quick Review: Yes       Request Review Reminder Emails: Never         Auto-Publish Inventory: Yes       Request Form: None Selected         Apply Policies to Inventory: Yes       Project Form: None Selected         Project Summary Emails: Never       Upload and Scan		
Project Metadata	View Project Metadata		
Aliased Projects	There is no aliased project for this project.		
Child Projects	There are no child projects for this project.		
Status	In Progress 💌		
Progress	Audit (does not include files within archives)         There are no scanned files for this project.         Inventory Review         There are no inventory items for this project.         Inventory with Legal / Remediation / Security Issues         There are no inventory items for this project.		

4. In the Advanced Options section, click Upload and Scan. Click Choose File and browse to the file or archive of files you want to upload. If uploading multiple files, ensure that they are placed into an archive of type zip, rpm, tgz or tar.gz prior to upload.

📁 Upload to Scan		
* File 🖪	Choose File MyFiles.zip	
* Action	Select an action	

5. To upload a file or archive without scanning, select **Upload** in the **Action** menu and click **Process** to start the upload.

The file or archive of files will be uploaded to the scan server into the directory specified by the uploadToScanUploadDirectory property.

Internal directories will be created based on the project ID and file name, as demonstrated in the following example:

• Single file—Upload of bar.dll as part of Project1 with ID 1. The file is uploaded to the directory:

/MyUploadDirectory/1/bar/bar.dll

• Archive of files—Upload of foo.zip containing 3 files as part of Project1 with ID 1:

/MyUploadDirectory/1/foo/foo1
/MyUploadDirectory/1/foo/foo2
/MyUploadDirectory/1/foo/foo3

If the uploadToScanUploadDirectory already contains a file or archive with the same name, the user will be prompted to overwrite the files with the new content.

🚯 Home   🎁 My Proje	ects   🗹 Requests   🚦 Policies   🕑 Scheduler   😲 Research   📈 Reports –	
💋 Upload to Scan		
* File 🗓	Choose File No file chosen	
* Action	×	
	Upload Only	Process Cancel
	Upload and Scan	Cancer

- 6. To upload a file or archive and automatically kick off a scan/report on the uploaded file do the following:
  - a. Select Upload and Scan in the Action menu.
  - **b.** When prompted, enter the name of the workspace to associate to the uploaded files to. Ensure that the name is unique in the system and follows standard naming conventions (e.g. does not include spaces or special characters).
  - c. Check off one or more reports to run with the scan, or leave unchecked to do a scan only.
  - d. Click **Process** when ready to start the upload and scan/report.
    - Single file: upload of bar.dll as part of Project1 with ID 1. The file is uploaded to the directory:

/MyUploadDirectory/1/bar/bar.dll

• Archive of files: upload of foo.zip containing 3 files as part of Project1 with ID 1:

/MyUploadDirectory/1/foo/foo1
/MyUploadDirectory/1/foo/foo2
/MyUploadDirectory/1/foo/foo3

🕤 Upload to Scan	
* File 🖪	Choose File MyFiles.zip
* Action	Upload and Scan
* Workspace	New Workspace 💙 myWorkspace
Reports 🖪	<ul> <li>Scanned Files Report</li> <li>Third-Party Indicators Report</li> <li>Palamida Analyzer - Quick Assessment</li> <li>Palamida Analyzer - Group Builder</li> </ul>

### Limitations

Upload and Scan has the following limitations:

- Every **Upload and Scan** function will create a new workspace. To scan the uploaded content as part of an existing workspace, use the **Upload Only** function and edit the workspace to point to the directory containing the uploaded content.
- Files uploaded using the **Upload to Scan** function may not be delete from the Web UI. To delete uploaded content, a system administrator must access the scan server file system directly, navigate to the upload directory and delete the files.
- In a multi scan server environment, only one scanner may be designated for **Upload to Scan** projects. Set the scan server alias of this scanner in core.properties.

### **Error Handling**

If there are unacceptable exceptions in any of the above steps, on either the core or scan server: The error message contains a short description only if that description does not provide security-sensitive information

If the error happened on the core server, then the error is logged in catalina.out on the core server. If the error happened on the scan server, then the error is logged in catalina.out on the scan server.

### **Security Features**

This section describes the security features in the Upload to Scan servers:

- Core Server
- Scan Server

### **Core Server**

User must be logged in to the FlexNet Code Insight application, which provides all the usual security benefits, including use of the CSRF Token.

User must be the project's owner or one of the project's auditors.

### **Core.properties**

If any of the following properties is unset (or set to bad values), this feature will not run:

- upload.to.scan.enable.core must be "true" (without quotes)
- upload.to.scan.max.file.size must be an integer greater than zero. It can be left black if you decide not to limit the size of the file.
- upload.to.scan.scanner.alias must be a string.

The core server handles all interactions with the user, the user will never directly access any scan server.

Uploaded files are managed by the core server as a simple array of bytes in memory (i.e., never written to disk), ensuring that potentially malicious files are never a threat to the core server.

User uploads files through the FlexNet Code Insight application, using the standard HTTP file transfer, because the user must not require additional physical permissions or special access on any FlexNet Code Insight server and must not require any software beyond the web browser they use to access the FlexNet Code Insight application

### Scan Server

The Scan Server has the following security features.

#### scanEngine.properties

If either of these properties are unset (or set to bad values), then this servlet will not run:

- uploadToScanEnableScanner must be "true".
- uploadToScanUploadDirectory must be a string.
- Must be equal to (or a child directory of) the directory defined in the serverFileSystemRoot property.
- The serverFileSystemRoot property is also set in the scanEngine.properties file.

Additional security features are:

- Scan server only accepts HTTP Post submissions, never HTTP Get submissions.
- All uploaded/extracted files are set to read-only and non-executable.
- All extracted directories are set to read-only and executable.
- On Linux systems, directories must be executable to be read.
- It will refuse to create symbolic links of any kind.

• Upload to Scan checks every file as it is extracted and written to see if that file is a symbolic link. If the file is a symbolic link, it is deleted and a line is written into the Scanner's log file:

[INFO] Upload to Scan (scanner): Successfully deleted symbolic link: " + filePath

where filePath is the full path to the symbolic link which was deleted. This process is identical for all uploaded files, whether the user uploads one file or uploads an entire archive.

• Extracted files will only be written into the uploaded file's parent directory or a child directory of the uploaded file's parent directory. This keeps the upload from writing any content to other locations on the file system (e.g., a malicious attempt to upload an app to the Tomcat webapps directory or an accidental attempt to overwrite the '/' directory).

Chapter 36 Upload to Scan

Using Upload to Scan