BLACK DUCK | PROTEX

System Administrator Guide
7.4

This edition of the *System Administrator Guide* refers to 7.4 of Protex.

This document created or updated on Thursday, July 14, 2016.

Please send your comments and suggestions to:

Black Duck Software, Incorporated
800 District Avenue
Suite 221
Burlington, MA 01803 USA

Contents

Preface

Target Audience

The target audience for this document is system administrators or individuals responsible for installing and maintaining the Protex environment.

General users should read the *Protex User Guide* and the online Help.

Related Documents

The documentation set for Protex consists of:

Title	File	Description
Protex Deployment Guide	Deployment_Guide.pdf	Information about designing, scheduling, and implementing a Protex deployment.
Protex Installation Guide	Install.pdf	Information about installing and uninstalling Protex.
Protex System Administrator Guide	SysAdmin.pdf	Information and reference materials for configuring and managing the Protex server.
Protex Getting Started Guide	GettingStarted.pdf	Information about using the Protex tutorial files.
Protex User Guide	User_Guide.pdf	Information and reference materials for using Protex.
Protex Release Notes	ReleaseNotes.pdf	Information about new features, changes to existing features, and fixed issues in each Protex release.
Protex Online Help	Online	Information and reference materials for using Protex.
SDK Release Notes	WhatsChanged.pdf	Information about new features, changes to existing features, and fixed issues in the Protex Software Development Kit (SDK).
How to Use the SDK Code Examples	Code_Examples.pdf	Information about how to install and use the Protex Software Development Kit.
Protex SDK Documentation	Online	Information and reference materials for the Protex Software Development Kit.
Protex SDK Javadoc	http://<Protexserver>/sdk-docs/index.html	Online access to the Javadoc created from the actual Protex SDK sources.

Customer Support

If you have problems with the software or the documentation, please contact Black Duck Customer Support.

For complete customer service options, refer to:

https://www.blackducksoftware.com/support/contact-support

You can contact Black Duck Support in several ways:

- From within Protex: **Tools** > **Admin Center Support**
- Online: http://customerhub.blackducksoftware.com
- Email: support@blackducksoftware.com
- Phone: +1 781.891.5100, ext. 5
- Fax: +1 781.891.5145
- Hours: Monday - Friday 8:00 - 18:00 Eastern Standard Time (US EST)

Note: Customers with an Enhanced Customer Support Plan can contact customer support 24 hours a day, 7 days a week to obtain Tier 1 support.

To access a range of informational resources, services and support, as well as access to Black Duck experts, visit the Black Duck Customer Success Portal at:

https://www2.blackducksoftware.com/support/customer-success

You can use the Internet to log Protex issues. To use this resource, a login and password are required. Login credentials for this service are emailed to you at registration. However, if you have not received this information, or you have misplaced or forgotten your password, please contact Black Duck Customer Support.

If you would like someone to perform Protex tasks for you, please contact the Black Duck Services group. They offer a full range of services, from planning, to implementation, to analysis. They also offer a variety of training options on all Black Duck products. Refer to https://www.blackducksoftware.com/services/ for more information.

Training

Black Duck training courses are available for purchase. Learn more at https://www.blackducksoftware.com/services/training.

View the full catalog of our online offerings: https://www.blackducksoftware.com/academy-catalog.

When you are ready to learn, you can log in or sign up for an account: https://www.blackducksoftware.com/academy.

Services

If you would like someone to perform Protex tasks for you, please contact the Black Duck Services group. They offer a full range of services, from planning, to implementation, to analysis. They also offer a variety of training options on all Black Duck products. Refer to https://www.blackducksoftware.com/services/ for more information.

Chapter 1: Protex System Administration

The administrator topics are written for Protex system administrators and managers. Administration topics are for anyone responsible for administering a Protex system.

Protex system administration covers a broad range of topics. Typical tasks for a Protex system administrator include the following:

- Initially configuring the Protex environment:
    - Registering your Protex license
    - Configuring LDAP authentication
    - Configuring Protex for SSL
- Creating and managing user accounts
- Adjusting server tuning and server system parameters
- Day-to-day Protex system administration:
    - Backing up data files (and restoring if necessary)
    - Managing disk space
    - Managing Solr indexes
    - Retrieving and installing Protex and KnowledgeBase updates

The topics covered in the *Protex System Administrator's Guide* are restricted to tasks that can be performed by users with the administrator role. Administration tasks that can be performed by users with the manager role, such as global configurations, are described in the *Protex User Guide* and the online Help.

The system administrator topics assume that you have already installed the Protex web application, and you have set up all networking software that you plan to use.

Note: The operations you can do within Protex are determined by your user role. If you do not have the proper role, the option is grayed-out and unavailable in your display. Most of the system administration tasks require the administrator role.

1.1 Protex Product Overview

Open source software (OSS) use has become more and more common as developers turn to it to reduce costs, enhance flexibility, and reduce time to market. But as organizations increase their use of open source, they need better solutions to logistical open source challenges.

Black Duck® Protex™ is a software application that provides visibility into the open source components used within your code base, throughout your development life cycle. Protex provides a way of reviewing code, seeking component and legal approvals, understanding license obligations, and creating reports helping you manage the open source software used in your code. By scanning and analyzing your software code, providing a bill of materials (BOM), and finding issues early in the development cycle or well in advance of a due diligence event, Protex helps you reduce business risks, complete software projects on time and on budget, and stay on track with your business goals.

Protex alerts developers, legal counsel, and management to intellectual property (IP) issues that arise during the software development process. Additionally, it provides a way to track the resolution of each issue, giving a clear, documented history to satisfy company compliance requirements. Protex creates a collaborative environment in which legal counsel and the development teams can efficiently access the information required to make timely business decisions.

Protex automatically discovers and identifies the origin of open source components in your code base, essential for enforcing license and other policy compliance. Protex helps you understand which licenses govern the modification, use, and distribution of the software in your code base. It facilitates the protection of your corporate intellectual property, assists with compliance and reporting, and identifies the use of licensed software in conflict with established licensing terms or your corporate policies. Protex enables the implementation of a repeatable business process to support corporate compliance policies.

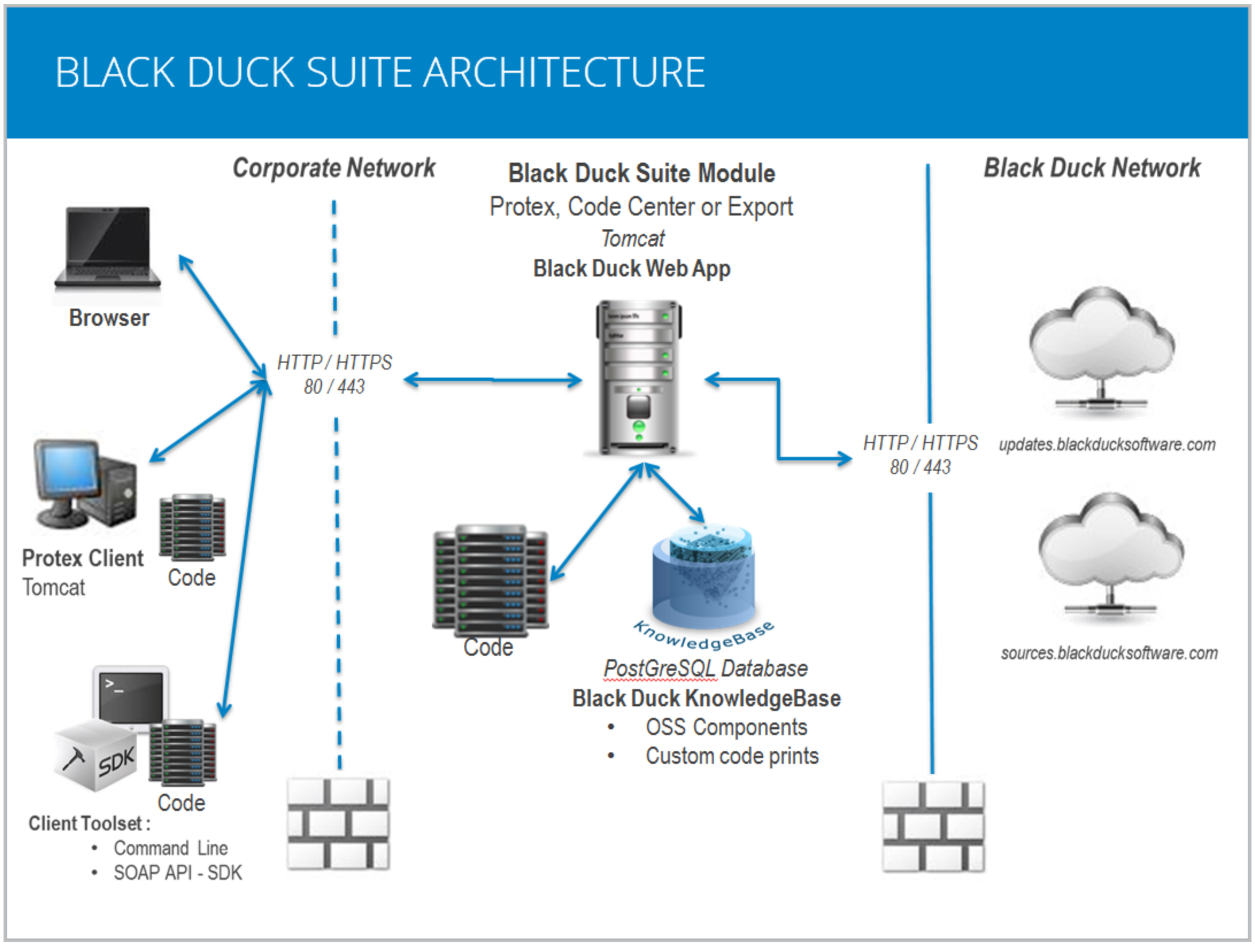
Protex manages the complexity of license obligations by providing accurate, up-to-date component and licensing information to legal counsel, developers, and managers. By enabling the proactive management of component software, Protex reduces personnel and development costs, improves time-to-solution, and makes delivery schedules more predictable.

1.1.1 Protex Architecture Overview

Black Duck Protex is an application that uses multiple components to perform the work of scanning and analyzing source code files.

The following figure illustrates a typical Protex system architecture.

Figure 1.1: Black Duck suite architecture



Protex Servers

Protex requires a dedicated server that should not be used for other business purposes. The hardware requirements are generally determined by the size of your code base, the frequency with which you scan your code base, and the number of concurrent users.

We recommend that Protex servers be co-located with your major source code repositories and build systems; in other words, in the same physical location, server room, or rack. This eases the integration process and minimizes network latency issues during scans. This is straightforward if your development and management takes place in a single location.

If your development and management takes place at multiple locations, you must consider where to locate the server and how to manage access. Some organizations maintain a central copy of all source code and manage their analysis at a central location. Others opt to decentralize the analysis, using the Protex client tool for scanning code from remote locations.

Protex Application Server

The Protex application server contains all components required to perform analysis, provided that the server can access your code repositories.

When you install the application server, the following components are installed:

- **Apache Tomcat** - Tomcat is a web application, a JSP (Java Server Pages) and servlets container. This component is supported and maintained as part of the Apache-Jakarta open source project. It includes many features that make it a useful platform for deploying web applications and web services. Protex uses a custom Tomcat sever; you cannot deploy Protex on another Tomcat instance.

Tomcat provides a setting for Java code to run in cooperation with a web server. It has tools for management and configuration and can be custom configured using XML files.

- **PostgreSQL database** - PostgreSQL is an open source database management system (actually an object-relational database server) released under a flexible BSD-style license. It provides an alternative to the proprietary database systems such as Oracle, Sybase, IBM DB2, and Microsoft SQL Server. Protex uses four separate databases to store the Black Duck KnowledgeBase and your data.

Protex Databases

The installer creates a PostgreSQL database on the Protex application server, and creates four databases to store KnowledgeBase and customer data.

Table 1.1: Protex databases

Database name	Description
bds_basic	(read-only) Contains product and standard KnowledgeBase information, including open source project and release information.
fp_basic	(read-only) Contains codeprint (fingerprint) information for the projects in the KnowledgeBase.
bds_customer	Contains customer configuration data, including Protex users and projects.
fp_customer	Contains customer codeprints; both custom codeprints and fingerprints.

Your local version of the Protex KnowledgeBase (`bds_basic` and `fp_basic`) contains information about thousands of licenses, and many thousands of codeprinted projects. You must maintain an active support subscription to receive KnowledgeBase updates.

Scan Repository

For Protex to scan your code, the code must be stored on the Protex application server or on a disk available to the application server.

Typically, code is retrieved from a source code management system and placed on a file system to run analysis. This file system is referred to as the **Scan Repository**. The files are not required to remain permanently on the scan repository and can be deleted after the scan. Your implementation can include both application server and local scan repositories.

- Repository is on the **application server**: In this case, the scan repository is on (or available to) the Protex application server itself, or on a device attached to the server. This is the recommended configuration for optimizing Protex performance, but works best in a centralized development environment or with local Protex application servers.

On Linux, the default location for the scan repository is `/home/blackduck`. You can configure this location. On Windows this is the root directory; Protex can access all drives on the Windows system.

- Repository is local (accessible from a local machine): The scan repository is on a local drive, which might be a desktop machine or a shared server. This configuration requires the use of the Protex client software to run an analysis. This configuration allows the Protex analysis to be run from remote locations, which works well in a decentralized development environment or with remote Protex servers.

In either case, the process of copying code from source code management to the scan repository should be repeatable, as this is a very important step in automating Protex for ongoing delta analysis of your code.

Protex Browser Requirements

The Protex user interface is HTML-based and requires a browser for access. Black Duck software tests the latest versions of available browsers during development. New browsers are continually being released, but are not always 100% backwards compatible. For a complete listing of tested and approved browser versions for this release of Protex, refer to Supported Browsers.

The following settings must be enabled for all browsers:

- **Cookies** - Protex uses cookies to check user authentication; verify that cookies are enabled in your browser.
- **Popups** - Your browser must allow popups from the Protex server and from localhost if you are accessing Protex using the client software.

Note: The minimum supported browser window size is 1024 x 768.

Note: Protex does not support Internet Explorer in compatibility mode.

Protex Client

Black Duck recommends that your Protex server and code repositories are in the same location, and that you upload a copy of your code to the Protex server. However, if your business has code repositories in multiple locations, or your code security needs prevent storing code on the Protex server, there is another option available to you.

You can use the Protex client for scanning code at a remote location from the Protex server. You can also use the Protex client to scan and analyze code that is not accessible from the Protex server; for example, code on a laptop or a remote machine. The Protex client software allows you to use the **File Comparison Tool** when identifying discoveries.

When running scans, Protex collects data from the scanned files to create the signatures required for matching. The read activity occurs in the code location: on the local client for client-side scans, and on the server for server-side scans. In the case of client-side scans, this data is sent over the network to the Protex server. Client-side scans require constant connection to the Protex application server since data is uploaded from one to three files at a time.

Note: The Protex client has a retry option. For example, if you experience connection timeout issues during long running scans, the client attempts to reconnect. After all files are uploaded to the server, you can disconnect the client and the analysis continues on the server.

The client installer also uses a Tomcat instance. On the client, Tomcat functions as a means of accessing your files on your local system. The web application acts as a proxy and sends information to the Protex application server. Tomcat allows the Protex client to access local system files, and to exchange information as required with the main application server.

Protex Connectivity Requirements

Protex has the following network and connectivity requirements:

- Connectivity to the Internet from the application server. Connection through a static proxy server is acceptable. Protex must be able to communicate with the following:

Table 1.2: Connectivity Requirements

URL	IP Address	Description
updates.protex.blackducksoftware.com	208.177.254.14	Black Duck Update server — Provides periodic software and KnowledgeBase updates to customers.
sources.blackducksoftware.com	208.177.254.10	Black Duck File Comparison Sources server — Used to provide read-only access to open source project code in the Black Duck KnowledgeBase for file comparison purposes.

- Connectivity to the application server and Internet from the internal clients through a static proxy is also acceptable.
- On Microsoft Windows Server 2008 systems, you must disable the Internet Explorer Enhanced Security Configuration option; otherwise, users of the Microsoft Internet Explorer browser cannot log in to Protex.

Note: Refer to http://technet.microsoft.com/en-us/library/dd883248(v=ws.10).aspx for more information.

The Protex application server has the following port requirements:

- 80 (default for HTTP), or 8080 (default for HTTP for non-root users)
- 389 LDAP port

- 443 (default for HTTPS), or 8443 (default for HTTPS for non-root users)
- 8005 Tomcat shutdown port
- 55432 PostgreSQL port

Note: If you have implemented a multi-server scan implementation, you may need to adjust your firewall settings to allow the scan servers to communicate with the application server through SSL using the PostgreSQL port.

1.1.2 Understanding the Protex User Interface

Protex v.7 introduced the Suite user interface. The Classic Protex user interface is being redesigned for improved usability. In future releases, features will be migrated from the Classic interface to the Suite interface. During the transition period, there may be more than one way to view data or perform a task within Protex.

Tip: If the documentation does not specify where you perform a procedure, you should assume that you perform it in the Classic interface.

The Suite interface offers a number of advantages:

- You can navigate between pages in Protex using the Forward and Back buttons in your browser.
- You can bookmark a project page using your browser's native bookmark function. For example, in Mozilla Firefox, go to **Bookmarks** > **Bookmark this page**. You can bookmark project pages, search results, and others.

Until the migration is complete, some tasks are only available in the Classic interface. Any action that you cannot perform in the new Suite interface will take you to the appropriate page in the Classic interface.

- To navigate from the Suite interface to the Classic interface:
  - From the **Browse** menu, select **Classic View**.
  - From your user name menu, select **Tools**.
- To navigate from the Classic interface to the Suite interface, click the Black Duck Protex logo in the header.

When you navigate between the two interfaces, each opens in a new browser window.

The interface displayed when you log into Protex depends on how you access Protex and how your administrator has configured Protex.

- By default, when you log in using the web application, the Suite dashboard displays, which contains summary graphs, charts, and a list of projects for which you have permission.
- If you log in using the Protex client, the Classic My Protex page displays, which contains a list of projects for which you have permission.
- If your administrator has disabled the Suite interface, the Classic My Protex page displays.

1.1.3 Support for Multi-Byte Characters

Protex server installations are supported only on English operating systems. During the installation, Protex sets the locale to en_US.UTF-8. All communications between Protex and the client are UTF-8 encoded.

Tip: Always save files containing multi-byte characters as UTF-8 instead of ASCII. Protex can scan files and folders containing multi-byte characters if the files are saved with UTF-8 encoding.

Protex also supports the use of multi-byte characters with UTF-8 encoding in the following areas of the user interface:

- Project names and source directory names
- Project and component descriptions
- Component comments on the **Identify** page
- File and folder comments on the **Identify** page
- The Report comment box

If Protex encounters characters that it cannot recognize as UTF-8, a warning message appears in the **Details** box of the **Analysis Complete** dialog box. In most cases, messages showing a few bytes of unrecognizable characters can be ignored, although you should investigate if larger portions of files are unreadable.

Chapter 2: Initial Configuration

This chapter contains information about how to perform the initial configuration for your Protex environment.

The majority of the procedures in this chapter should only need to be performed once, during the initial setup of your Protex environment.

2.1 Registering your Protex License

Protex requires the system administrator to register your license prior to use.

You must register Protex prior to use. Typically, this is done at installation time. You only have to register once, and any subsequent software updates automatically update your license.

The Protex license can be based on elapsed time (such as three months), or a number of seats. The **Detailed Product Registration Report** shows you how much longer your registration is in effect, and displays a warning if you are getting close to expiration.

> **Note:** Before you begin this operation, you need a registration key, which is sent to you by Black Duck.

To register your license:

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Admin Center** > **Registration**.
4. If necessary, select **General** from the **Show:** filter. The **Registration** page displays three sections, as follows:
    - **Edit local registration settings** - This section contains: The registration ID (registration key), external access protocol information, last renewed date, and last renewal attempt.
    - **Edit external access proxy settings** - This section contains: proxy setting sharing value, proxy type (can be secure HTTPS), proxy host, proxy port, proxy username field, and proxy password value if applicable.
    - **Edit mail settings** - This section contains: The administrator address, SMTP mail server name, mail from address, SMTP username, and password details.
5. In the **Registration ID** field, enter your registration key.

6. In the **External access protocol** drop-down, select HTTP or HTTPS.
7. Click **Renew Registration**.

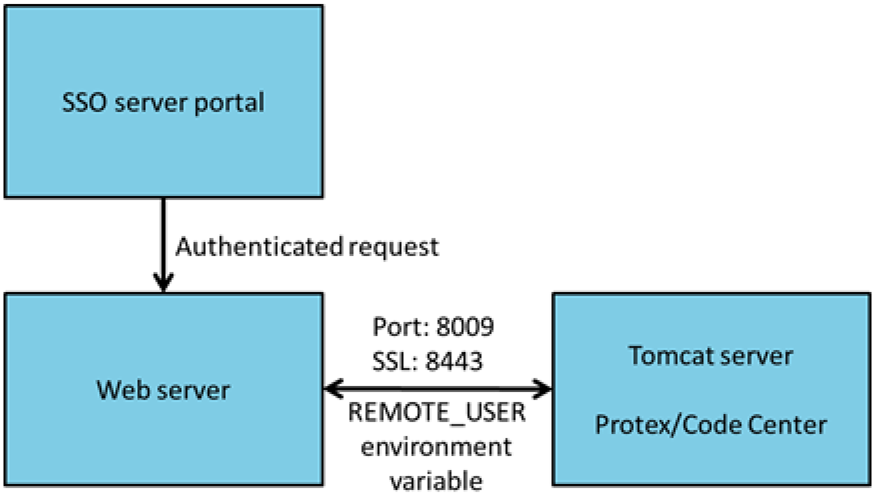
2.2 Single Sign On Overview

Black Duck supports the following configuration to address customers' requests to integrate their enterprise single sign on (SSO) implementations with current releases of the Protex and Code Center products.

Note: Black Duck will work to improve support for SSO integrations in future releases.

SSO authentication works by letting the Black Duck applications know the trusted information to find in the HTTP request, assuming that this request has already been authenticated by the SSO infrastructure sitting in front of the application. You can use existing HTTP-based SSO infrastructures, such as those offered for the Apache web server.

In an enterprise environment, a user typically logs in to the corporate SSO portal, which authenticates the user. The web server creates a header from the authentication information and forwards the request to the Apache Tomcat web server running the Black Duck application. Once the authentication is complete, the web server routes the user through to the Black Duck application running on the Apache Tomcat web server. The user never sees a log in page for the Black Duck application.



To enable SSO for Black Duck applications, you must let the application know that it is running behind a secure HTTP server that forwards trusted requests to it, then tell it where in the request to look for trusted authentication information. The Black Duck applications expect the SSO user name to come from `ServletRequest.getRemoteUser()`, which is the value of the `REMOTE_USER` environment variable (CGI variable in the Apache web server). The Black Duck application assumes that requests coming in are already authenticated and that there is a pre-established mechanism for extracting authenticated user information from incoming requests.

Note: Black Duck does not provide specific implementation details for any SSO tool. It is the customer's responsibility to determine how to configure their SSO tool to provide the needed information to authenticate the user to Black Duck applications.

Note: SAML is not supported.

2.2.1 Enabling SSO Authentication

✱ **To enable SSO authentication for Black Duck applications on Apache Tomcat web servers:**

1. On the Apache Tomcat web server where the Black Duck application is running, open the `tomcat.start` file for editing.

    - For Protex, this file is located in:

      Linux: `opt/blackduck/protexIP/config/bds-protexIP-tomcat.start`

      Windows:
      `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\protextc\Parameters\Java\`

2. To make the **External User ID** field visible on user account pages in the Black Duck application, in the `tomcat.start` file, set the system property `blackduck.sso-enabled` to true:

    Linux: `export JAVA_OPTS="-Dblackduck.sso-enabled=true ${JAVA_OPTS}"`

    Windows: `-Dblackduck.sso-enabled=true`

3. To disable form-based user authentication in the Black Duck application, in the `tomcat.start` file, set the system property `blackduck.web.disable-form-login` to true.

Linux: `export JAVA_OPTS="-Dblackduck.web.disable-form-login=true ${JAVA_OPTS}"`

Windows: `-Dblackduck.web.disable-form-login=true`

4. In Linux, save your changes to the `tomcat.start` file. In Windows, save and close the Registry Editor.

5. On the Apache Tomcat web server where the Black Duck application is running, open the `server.xml` file for editing.

    - For Protex, this file is located in:

      `/opt/blackduck/protexIP/tomcat/conf/server.xml`

6. Make the following changes in the `<Service>` section of the `server.xml` file:

    ```
    <Connector port="8009" enableLookups="false" redirectPort="8443"
    tomcatAuthentication="false" protocol="AJP/1.3"
    proxyName="proxy-server.domainname" />
    ```

    Note: If you are using the AJP connector over SSL, use Connector port="8443" instead of Connector port="8009."

7. Save your changes to the `server.xml` file.
8. Restart the Apache Tomcat web server.
9. Create or edit Protex users with the `External User ID` set to the user name coming from the SSO system; for example, the `SM_USER` value coming from CA SiteMinder.
10. Configure the web server to map login URLs to the Black Duck application. For example:
    - `login/protex` to forward users to Protex

2.2.2 Customizing Your SSO Logout Page

If you are using single sign-on (SSO), you can specify where the user is directed when they log out of Protex. If you do not specify a custom logout page, the user is redirected to the Protex login page. This is the default behavior.

✱ **To customize your SSO logout page:**

1. On the Apache Tomcat web server where the Black Duck application is running, open the `tomcat.start` file for editing.
    - For Protex, this file is located in:

      Linux: `opt/blackduck/protexIP/config/bds-protexIP-tomcat.start`

      Windows:
      `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\protextc\Parameters\Java\`
2. Add the following command. Replace the URL in the example with the URL of the page to which you want users directed upon logout.
    - Linux: `export JAVA_OPTS="-Dblackduck.sso-logout-page=http://www.example.com ${JAVA_OPTS}"`
    - Windows: `-Dblackduck.sso-logout-page=http://www.example.com`
3. In Linux, save your changes to the `tomcat.start` file. In Windows, save and close the Registry Editor.
4. Restart the Apache Tomcat web server.

2.3 Using LDAP Authentication

Lightweight Directory Access Protocol (LDAP) allows querying and modifying directory services from a common, central location. It is used to provide user and group lookups and various other types of information. Protex supports user authentication using LDAP servers instead of saving this information in its own servers.

The ability to use LDAP authentication in Protex is set on a per-user basis. For each user that you want to authenticate using LDAP instead of using their Protex password, you must set a flag on their account and also provide their LDAP login ID.

Tip: Configuring an LDAP solution is an advanced procedure that should be completed by your LDAP Administrator.
To complete this task, it may help to use an LDAP browser such as JXplorer to examine your current LDAP server settings. See http://www.jxplorer.org/ for download information.

A constructed DN (Distinguished Name) is used to find the user in the LDAP tree and authenticate the given password against the one stored in the LDAP server. There are two authentication methods supported:

- Bind Authentication — Authentication directly to the LDAP server.
- Password (hash) Comparison — The user password is compared with the one stored in the repository. This is done by retrieving the password attribute and checking it locally, or by performing an LDAP *compare* operation. The password comparison method sends the password provided to the server for comparison, and the real password value is never retrieved.

You can use either MD5 or SHA1 password encoding.

2.3.1 LDAP Fields

This section describes the fields used to configure LDAP for a particular site. The fields are set in the file: `<INSTALL_DIR>/config/custom.properties`. For example, for a default Linux installation, this is: `/opt/blackduck/protexIP/config/custom.properties`. This is a standard Java properties file, and each field is set using the *key* = *value* syntax.

Table 2.1: LDAP Fields

Key	Value	Description
ldap.authenticationEnabled	true OR false	Whether or not to allow LDAP authentication for this server. If false, all other fields are ignored.
ldap.providerURL	ldap://host:port/base_dn	The URL of the LDAP server, including host name, port (defaults to 389), and the baseObject from which to start all user lookups.
ldap.authenticationType	authentication type	The type of authentication used to establish the initial directory context. See http://java.sun.com/products/jndi/tutorial/ldap/security/auth.html for the available values.

ldap.dirContextFactory	`initialDirContextFactory`
	OR
	`initialAnonymousDirContextFactory`
		Describes how to log in to the LDAP server. If `initialDirContextFactory` is used, then the manager DN and Password parameters must also be provided. Otherwise, anonymous login is used.

ldap.managerDN	username	The username that Protex uses to log in to the LDAP server.
ldap.managerPassword	password	The password that Protex uses to log in to the LDAP server.
ldap.searchBase	DN with wildcard	The base DN from which the search for users should be performed. An example is `ou=people,ou=company`.

Key	Value	Description
ldap.searchFilter	User Pattern	User Pattern used at login time. An example is `cn={0}`.
ldap.userDNPattern	User Pattern	The relative Distinguished Name (DN) pattern to which the search base is appended. Users' DNs are constructed by replacing the placeholder `{0}` with the username supplied by the user during authentication. An example pattern is `uid={0}, ou=developers` where a search base of `dc=mycompany,dc=com` is appended to form an absolute DN.
ldap.userLogin	User Pattern	This field is deprecated and is no longer used by Black Duck products. You can delete it or comment it out.
ldap.passwordEncoder	password encoder	The SHA1 password encoder used by the `ldapPasswordAuthentication` bean. `blackduckLdapShaPasswordEncoder` and `blackduckLdapMd5PasswordEncoder` are recommended
ldap.authenticatorBean	`ldapBindAuthentication` OR `ldapPasswordAuthentication`	Which authentication type to use.
ldap.groupSearchBase	subtree	The base DN from which the search for group membership should be performed.
ldap.groupRoleAttribute	attribute type	The ID of the attribute that contains the role name for a group.
ldap.bindAttribute	attribute type enumeration of `{dn, sAMAccountName}`. Automatically defaults to `dn`. This is not case sensitive.	The attribute type to be used for binding with the LDAP server. For most servers the default `dn` will suffice. However, for Active Directory 2003 under DIGEST-MD5 authentication type, `sAMAccountname` is required.

2.3.2 Configuring LDAP on the Protex Server

The following is a sample `<INSTALL_DIR>/config/custom.properties` file for Protex version 4.5 and later.

```
#OpenLDAP properties file
# Whether or not to support authenticating users via LDAP
ldap.authenticationEnabled = true

# URL of the LDAP server: String of the form
# <code>ldap://host:port/base_dn<code>
ldap.providerURL = ldap://10.12.13.89:389/
```

```
# If your LDAP server allows anonymous searches, then set the
# following variable to "initialAnonymousDirContextFactory"
ldap.dirContextFactory = initialDirContextFactory

# The type of authentication used to establish the initial directory
# context. See
# http://java.sun.com/products/jndi/tutorial/ldap/security/auth.html
# for the available values.
ldap.authenticationType = simple

# If your LDAP server does not allow anonymous searches then you
must
# provide a "manager" user's DN for login
ldap.managerDN = cn=Joe Duck,ou=IT,dc=blackducksoftware,dc=com

# The manager user's password. Leave it blank if you are using
# ldap.managerEncryptedPassword instead.
ldap.managerPassword = bdssamplepwd

# The base DN from which the search for users is performed.
# An example is "ou=people,ou=company,dc=domain,dc=com".
ldap.searchBase = ou=Development,dc=blackducksoftware,dc=com

# The pattern which is searched.
# If employeeNumber is defined as unique key, but login uses uid or
cn instead
# An example is "employeeNumber={0}"
ldap.searchFilter = cn={0}

# Pattern used at login time
ldap.userLogin = cn={0}

# The password encoder used by the ldapPasswordAuthentication bean
ldap.passwordEncoder= blackduckLdapPasswordEncoder
```

```
# The type of LDAP authentication to use: either
"ldapBindAuthentication"

# or "ldapPasswordAuthentication"

ldap.authenticatorBean = ldapBindAuthentication


# The base DN from which the search for group membership is

# performed.

ldap.groupSearchBase = cn=users,dc=blackducksoftware,dc=com


# The ID of the attribute containing the role name for a group

ldap.groupRoleAttribute = cn


#End OpenLDAP properties file
```

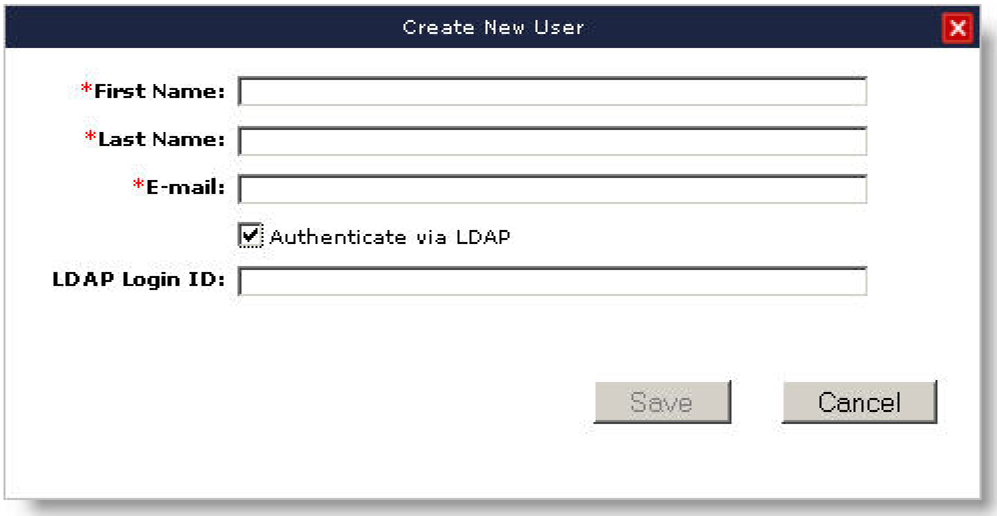
After the `/opt/blackduck/protexIP/config/custom.properties` file has been created and saved, you must stop and re-start the Protex Tomcat process

```
/etc/init.d/bds-protexIP-tomcat stop

/etc/init.d/bds-protexIP-tomcat start
```

2.3.3 Configuring a User for LDAP Authentication

After configuring LDAP in the `custom.properties` file and restarting Tomcat, you can now specify that a user must be authenticated using LDAP. Go to **Tools** > **User Accounts**. If you are adding this feature to an existing user, select their name from the list. Otherwise, click **Create New User**.

Figure 2.1: Create a New User who is Authenticated with LDAP



*First Name:

*Last Name:

*E-mail:

☑ Authenticate via LDAP

LDAP Login ID:

All users need a first and last name, and an email address. Once you click **Authenticate via LDAP**, the password fields either disappear or are disabled. Enter the LDAP login ID for the user. If you leave the LDAP Login ID field blank, the account is created as a non-LDAP account. However, in that case the user cannot log in because the account has no password.

Tip: If this is a new user account, remember to also assign the appropriate Protex roles before leaving this section of the **Tools** area.

If you encounter difficulties logging in with this new Protex user, all error message are logged in the following location on the Protex server: `/opt/blackduck/protexIP/tomcat/logs/blackduck_log.txt`.

2.3.4 Enabling LDAP Case Insensitivity

As of Protex 7.4, you can specify case insensitivity for your LDAP username authentication.

✱ **To enable LDAP case insensitivity:**

1. Log in to Protex as an administrator user.
2. In the upper right panel, click **Tools**.
3. On the **Tools** page, under **Settings**, click **Policy Manager**.
4. At **Policy Manager** > **General** > **Access**, click the check box for **Allow Case Insensitive LDAP Login**.
5. Click **Save**.
6. The **Policy Information Updated** confirmation message displays.

Note: LDAP case insensitivity cannot be enabled if duplicate IDs exist. If duplicate IDs exist, the **Duplicate LDAP users found** message displays. You must remove all duplicate IDs, then enable LDAP case insensitivity.

2.4 Configuring SSL Encryption on the Server

The Secure Socket Layer (SSL) allows secure communications between browsers and web servers. The data sent is encrypted by one side, transmitted, and then decrypted by the other side before processing. Both the server and the browser encrypt all communication packets before sending out data.

Besides encryption, SSL also provides client authentication on initial communications between the server and the browser. The server sends, and may request, certificates from the browser. This ensures proof that the site is who and what it claims to be. See the Tomcat website (https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html) for more information.

Tip: As a best practice, you should update your SSL encryption protocol on a regular basis to keep current with fixes for known vulnerabilities. For example, if you are using OpenSSL versions 1.0.1 through 1.0.1f, you should upgrade to a version that fixes the Heartbleed vulnerability reported in April 2014.

Protex uses the PKCS12 keystore format.

Although the Tomcat server runs on your internal network, you may want to enable SSL encryption to protect communication between the server and browsers. The process involves four phases, as follows:

1. Get a certificate from a third-party provider (for example, GoDaddy.com).
2. Import the certificate.
3. Upload the keystore to the Tomcat server.
4. Update the product registration.

This section provides an overview on how to do this.

Step I: Get a Certificate

To get a certificate:

1. At the command line, generate a SSL key and certificate signing request (CSR) using the following command:

```
openssl genrsa -out <keyfile> <keystrength>

openssl req -new –key <keyfile> -out <CSRfile>
```

Example:

```
openssl genrsa -out server.company.com.key 1024

openssl req -new -key server.company.com.key -out server.company.com.csr
```

This example creates a request for server.company.com to get a certificate signing request (CSR) from the signing authority.

> **Note:** It is important that the name entered for your server is the full host name on which your SSL server resides, and that the organization name is identical to the value in the *whois* record for the domain.

2. Send the CSR to the key signing authority; this is usually done through their web interface. Choose `Apache` as the web server type. Pay for their service and wait for them to send you a signed certificate.

The signing authority may ask for detailed information regarding your organization. They verify the information you provided to see if it matches with your domain registry information.

Step 2: Import the Certificate

To import the certificate to the keystore format used by the Tomcat server:

Once you receive a signed certificate, you must import it to the Tomcat server. Tomcat uses a keystore for holding certificates and keys. Note that the keystore can be stored in any file, but in this example it is called `.keystore`. What was generated earlier and what was received from your key signing authority is in a standard format that must be converted to *pkcs12* format.

No Chain Example:

If your certificate was not formed by a chain, use the following syntax to convert the format:

```
openssl pkcs12 -in <certificate> -inkey <key> -export -out
/root/keystore.tomcat -name tomcat -passout pass:changeit
```

For example:

```
openssl pkcs12 -in server.company.com.crt -inkey
server.company.com.key -export -out /root/keystore.tomcat -name
tomcat -passout pass:changeit
```

Chain Example:

If your certificate is formed by a chain (such as those created by GoDaddy.com), use the following syntax:

```
openssl pkcs12 –export –chain –CAfile –in <certificate> -inkey <key>
-out \

.keystore -name tomcat –passout pass:<password>
```

For example:

```
openssl pkcs12 –export –chain -CAfile gd_bundle.crt -in
server.company.com.crt -inkey server.company.com.key -out .keystore
-name tomcat –passout pass:changeit
```

In both cases, the password must be entered as the password for the certificate key. If you do not enter a password in the command, Tomcat prompts you for it.

The crt file is named differently depending on the issuing registrar. Also, this example uses the default key password used by Tomcat, which is *changeit*. This might be different on your system.

Step 3: Upload the Keystore - Linux

✱ To upload the keystore to the Tomcat server:

1. Upload the `.keystore` file to the /root directory on your Tomcat server.
2. Open the `/opt/blackduck/protexIP/tomcat/conf/server.xml` file on your server. This file defines the port that users use to connect to Protex. You see the definition of the default port 80.
3. Create a new connector port with the following information. You can copy-and-paste your existing HTTP port information and add the highlighted lines from this example. Change the port number to 443, which is the default HTTPS port.

```
<Connector port="443" URIEncoding="UTF-8"

     disableUploadTimeout="true"

     connectionTimeout="1200000"

     maxThreads="200"

     maxSpareThreads="4"
```

```
      maxKeepAliveRequests="-1"
      maxHttpHeaderSize="65536"
      compression="on"
      compressionMinSize="2048"
      scheme="https"
      secure="true"
      keystoreFile="/root/.keystore"
      keystorePass="changeit"
      keystoreType="PKCS12"
      SSLEnabled="true" />
```

4. (Optional) Depending on your system requirements, you have several options on what to do with the old port. You could ignore it, disable it, delete it, or redirect it. This example modifies port 80 to automatically redirect to the new port 443. This way, users do not need to change the way they access Protex. Add the following lines to the bottom of the default (port 80) connector definition:

```
<Connector port="80" URIEncoding="UTF-8"
.
.
.
   redirectPort="443"
   scheme="https" proxyPort="443" />
```

5. Restart Tomcat (as root), using the following command:

```
/etc/init.d/bds-protexIP-tomcat restart
```

Step 3: Upload the Keystore - Windows

✱ To upload the keystore to the Tomcat server:

1. Upload the `.keystore` file to the following directory on your server:

   ```
   C:\Program Files\Black Duck
   Software\protexIP\config\blackducksoftware.keystore
   ```

2. Open the `server.xml` file. The default location for this file is:

   ```
   C:\Program Files\Black Duck Software\protexIP\tomcat\conf
   ```

   This file defines the port that users use to connect to Protex. You see the definition of the default port 80.

3. Create a new connector port with the following information. You can copy and paste your existing HTTP port information and add the highlighted lines from this example. Change the port number to 443, which is the default HTTPS port.

```
<Service name="Catalina">
```

```
<Connector port="443" URIEncoding="UTF-8"

     disableUploadTimeout="true"

     connectionTimeout="1200000"

     maxThreads="200"

     maxSpareThreads="4"

     maxKeepAliveRequests="-1"

     maxHttpHeaderSize="65536"

     compression="on"

     compressionMinSize="2048"

     scheme="https"

     secure="true"

     keystoreFile="C:\Program Files\Black Duck
     Software\protexIP\config\blackducksoftware.keystore"

     keystorePass="changeit"

     keystoreType="PKCS12"

     SSLEnabled="true" />
```

4. *Optional:* Depending on your system requirements, you have several options on what to do with the old port. You could ignore it, disable it, delete it, or redirect it. This example modifies port 80 to automatically redirect to the new port 443. This way, users do not need to change the way they access Protex. Add the following lines to the bottom of the default (port 80) connector definition:

```
<Connector port="80" URIEncoding="UTF-8"

.

.

.

   redirectPort="443"

   scheme="https" proxyPort="443" />
```

5. Restart the Black Duck Protex Tomcat service.

Now, any communications between the port on the server and client are encrypted using SSL. If you completed the optional step above, then connections to HTTP are automatically redirected to use https://<*myProtexServer*>:443. See Configuring Tomcat to Run on a Different Port on page 32 for more information about changing your default port numbers.

Step 4: Update Local Registration Settings

✱ To modify the local registration settings to reflect the use of the HTTPS protocol: Log in to Protex.

1. From the username menu in the Suite interface, select **Tools**.
2. In the Classic interface, select **Tools** > **Admin Center** > **Registration**.

3. In the **Registration ID** field, enter your registration key.
4. In the **External access protocol** drop-down, select https.
5. Click **Renew Registration**. Protex refreshes the page with your changes.

2.5 Configuring Client Proxy Settings

Enterprise customers require proxy configurations as part of their secure environment. The proxy server acts as a security barrier by monitoring all traffic between the Intranet and the Internet.

Protex must be able to contact Black Duck Software for updates, registration, and to view code comparisons from the KnowledgeBase. You must enter the appropriate proxy connection details for the product to get past your company's firewall.

The normal configuration assumes that your client systems and the local Black Duck server use the same proxy settings. If this is not true, you can set some properties on your client system so that it works with local proxy settings. The section that follows outlines this procedure, which is accomplished through the Protex graphical user interface.

Proxy Configuration Prerequisites

Verify that you have the Black Duck Client tools installed on your system. Remember that system proxy settings are accessed in different ways on various platforms. The examples that follow give details for the specified platform.

> **Note:** Proxy and username are only required if the proxy requires authentication.

✱ To get the Linux Client proxy settings in Firefox:

1. Launch Firefox.
2. Click **Tools** > **Options** > **Advanced** > **Network** > **Settings**. The **Connection Settings** panel opens.
3. Record all information, including the host, port, and authentication.

✱ To get the Windows Client proxy settings in Internet Explorer:

1. Launch Internet Explorer.
2. Click **Tools** > **Internet Options**. The **Internet Options** dialog opens.
3. Choose the **Connections** tab.
4. Click **LAN Settings**. The **LAN Settings** dialog opens.
5. Record all information, including the host, port, and authentication.

> **Note:** If you are using an automatic proxy configuration script, work with your local networking management people to determine the value for your local proxy.

✱ **To configure the proxy settings:**

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Admin Center**.
4. Click the **Registration** tab.
5. In **Edit external access proxy settings**, enter the following information:
   - In the **Proxy setting sharing** field, select a value from the menu:
     - **unshared** - Select to only configure settings on the server.
     - **shared with clients** - Select to share the proxy settings with Protex clients. When users download the client, they also download a copy of the master `client.properties` file from the Protex application server. Note that after enabling this setting, you may still need to complete Configuring Default Client Settings for other properties.
   - In the **Proxy type** menu, select a value:
     - **http** - Hypertext Transfer Protocol: HTTP is a set of standards that is the default method of communication for web pages and web applications. HTTP is not a secure communications protocol. HTTP URLs begin with `http://` and use port 80 by default; it also commonly utilizes port 8008 or 8443.
     - **https** - Hypertext Transfer Protocol Secure (HTTPS) adds SSL/TLS (Secure Socket Layer/Transport Layer Security) to standard HTTP communications protocol. All data sent over HTTPS is encrypted before it is sent, this prevents anyone from reading that information if intercepted. HTTPS URLs begin with `https://` and use port 443 by default.
     - **socks** - Socket Secure (SOCKS) is an internet protocol for handling client-to- server requests and communications made through a proxy server. In addition, SOCKS5 provides authentication; only authorized users may access a server.
   - In the **Proxy host** field, enter the name of your proxy host.
   - In the **Proxy port** field, enter the proxy port number.
   - In the **Proxy username** field, enter a username.
   - In the **Proxy password** field, enter the password for the specified user.
6. Click **Set proxy options**. Protex refreshes the page with your changes.

   If you have more than one client installed, you may have to change the MIME extensions to point at the correct client.

2.5.1 Configuring Default Client Settings

If you have configured your Protex proxy settings to share settings with clients, when downloading the client tools (the Protex client or **bdstools**), you also download a copy of the master `client.properties` file from the Protex application server. The `client.properties` file lets you configure settings on the Protex client. However, during an online update, changes to `downloads/client/client.properties` are copied to `config/client.properties`, overwriting any custom configuration settings that you may have specified for your client.

As a best practice, you should create a `client-override.properties` file on the Protex application server to store custom settings that you want to enable on all clients; for example, `blackduck.scan.nThreads=5`. When users download components of the client tool set, they also download the `client-override.properties` file, which overrides default settings installed by an update.

Note: You must enable this setting in the Classic user interface. Go to **Tools** > **Admin Center** > **Registration** and under **Edit external access proxy settings**, set **Proxy setting sharing** to **shared with clients**.

Create the `client-override.properties` file in the following directory on the Protex application server:

```
/opt/blackduck/protexIP/config/client-override.properties
```

Note: This file is used by both the Protex client and **bdstool**.

2.6 Configuring Tomcat to Run on a Different Port

There may be times when you want to run the Protex Tomcat server on a port other than port 80. This section outlines how to make this modification.

Changing ports involves modifying two configuration files and changing the port number in the URL.

✱ To run Protex on port “1234”:

1. Log in as root.
2. Edit the following file:

   ```
   /opt/blackduck/protexIP/tomcat/conf/server.xml
   ```

3. Edit this line:

   ```
   <Connector port="80" />
   ```

   To read:

   ```
   <Connector port="1234"/>
   ```

4. Save your changes.
5. Open the second file:

   ```
   /opt/blackduck/protexIP/config/bds-protexIP-tomcat.start
   ```

6. Locate the line `export JAVA_OPTS`.

Note: On Windows, the Tomcat startup settings are configured in the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software
Foundation\Procrun 2.0\protextc\Parameters\Java\
```

7. Locate the statement `blackduck.baseURL=http://127.0.0.1:80`.
8. Change `80` to your new port number.

```
-Dblackduck.baseURL=http://127.0.0.1:1234/
```

9. To open the localhost homepage, enter the following URL in your browser:

```
http://127.0.0.1:1234
```

Note: If you have already installed Protex and want to make the change, restart the Tomcat service after you edit the `server.xml` and `/opt/blackduck/protexIP/config/bds-protexIP-tomcat.start` files. Log in to the server as root and issue this command: `/etc/init.d/bds-protexIP-tomcat restart`.

2.7 Changing the Default Path of the Scan Repository

For Protex to scan your code, it must be stored on the Protex application server or on a disk available to the application server. The default location for the scan repository is:

Linux - `/home/blackduck`

Windows - either the system property `USERPROFILE`

or `C:/Documents and Settings/blackduck`

You can configure Protex to use a different directory on the Protex server.

✱ To configure the location of your scan repository:

1. On your server, navigate to the Tomcat startup file.

   ```
   /opt/blackduck/protexIP/config/bds-protexIP-tomcat.start
   ```

2. Open the file with a text editor.
3. Add the following text to the end of the file to specify the location of your code repository on your Protex server:

   ```
   export JAVA_OPTS=" -
   Dblackduck.serverFileURL=file:///<firstPathElement>/<secondPathElement>/
   $ {JAVA_OPTS}"
   ```

Note: On Windows, the Tomcat startup settings are configured in the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software
Foundation\Procrun 2.0\protextc\Parameters\Java\
```

4. Save the file.
5. Restart Tomcat on the server.

2.8 Configuring Multi-threaded Processing

When running your server on a multi-core processor, the Protex analysis runs as a multi-threaded process. Testing has shown significant speed increases are possible, depending on your environment. Performance is based on a variety of factors including the number of concurrent scans, user activity, and the size of your projects.

This feature can also be disabled if you do not have a dedicated server and do not want Protex to use all your system resources. Contact Black Duck Customer Support for more information.

Typically, you should allow Protex to automatically choose the number of processes and the size of the thread pool. However, it is possible to adjust this feature based on your system requirements. There are two Tomcat startup parameters controlling this feature:

```
-Dblackduck.bom.pool.numThreads
```

The default value is the number of logical cores plus one:

```
Runtime.getRuntime().availableProcessors() + 1
```

```
-Dblackduck.bom.pool.queueCapacity
```

The default value is 3 times the number of processes (`numThreads`) as set above.

2.9 Configuring Email Settings

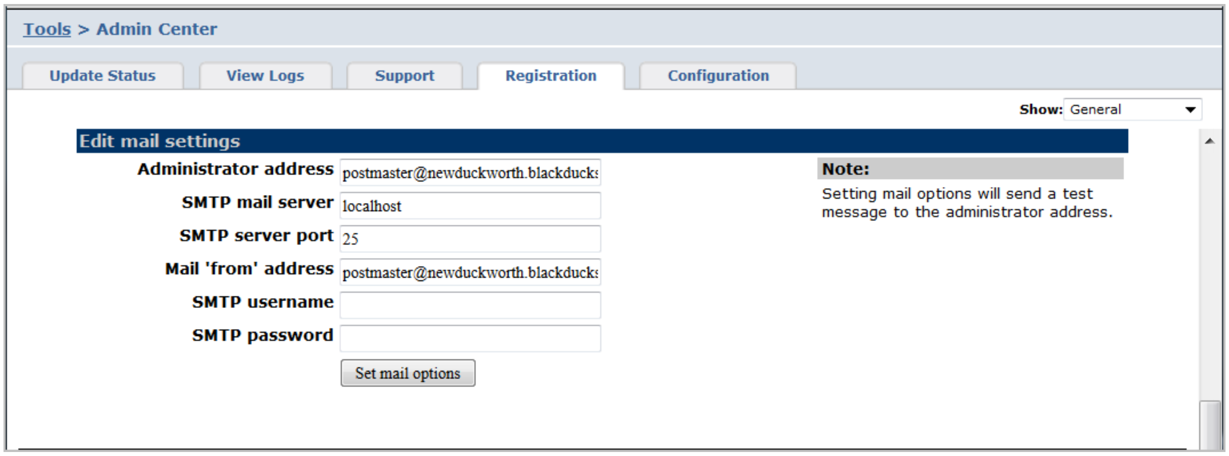
You must configure the Protex server before Protex can generate automated email messages. After configuring Protex for email, the following features can be enabled:

- The Protex server can send mail to a system administrator after an automatic upgrade.
- Protex can send reports to the specified email address after you run **Express Scan**.

✱ **To configure email settings:**

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Admin Center**. The **Update Status** page opens.
4. Click the **Registration** tab. The **Registration** page opens.

Figure 2.2: Tools > Admin Center > Registration page



Show: General

Edit mail settings

Administrator address: postmaster@newduckworth.blackducks
SMTP mail server: localhost
SMTP server port: 25
Mail 'from' address: postmaster@newduckworth.blackducks
SMTP username:
SMTP password:

Note: Setting mail options will send a test message to the administrator address.

5. In the Edit email settings section, enter the following information:
    - In the **Administrator address** field, enter the email address for the System Administrator.
    - In the **SMTP mail server** field, enter the host name of your mail server.
    - In the **SMTP server port** field, enter the port for the mail server.
    - In the **Mail 'from' Address**, enter the address that mail should be sent from.
    - In the **SMTP username** field, enter a username.
    - In the **SMTP password** field, enter a password, if required.
6. Click **Set mail options**.

Note: An additional step is to set `-Dmail.smtp.auth=true` in `/etc/sysconfig/bds-protex-tomcat`.

If `mail.smtp.auth=true`, Protex follows the authentication protocol specified in RFC 2554 (http://www.ietf.org/rfc/rfc2554.txt) regardless of whether the SMTP server requires it. For example, if you try to authenticate to exchange.blackducksoftware.com with an invalid SMTP username or password, it will fail. If you try to mail to a non-blackducksoftware.com address through exchange.blackducksoftware.com without authenticating using a valid SMTP username and password, it will also fail. If you try to mail to any address through exchange.blackducksoftware.com with a valid SMTP username and password, it will succeed.

If `mail.smtp.auth=false`, then mail sent through exchange.blackducksoftware.com will succeed only if it is being sent to a blackducksoftware.com address.

2.10 Configuring the Protex Dashboard

Protex 7 introduced a new user interface. Over a series of forthcoming releases, the Classic Protex interface is going to be redesigned for improved usability as various features are moved to the new Suite user interface. While we strongly recommend that you adopt the new Suite interface to take advantage of new features, we have provided the option that lets you configure Protex to launch with the Classic dashboard instead of the new Suite dashboard.

> **Note:** If you choose to launch Protex with the Classic dashboard, you should be aware that the Protex documentation for all tasks assumes that the user starts at the new Suite dashboard. This may cause confusion for new users who access the online Help for assistance when performing tasks.

The dashboard users see when they log in is controlled by a Tomcat startup parameter. To disable the new dashboard, you must start Protex using a special parameter. You can make the following addition to your Tomcat `/opt/blackduck/protexIP/config/bds-protexIP-tomcat.start` file:

```
-Dblackduck.ui.legacy.default=true
```

> **Note:** On Windows, the Tomcat startup settings are configured in the following Windows Registry key:
>
> ```
> HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software
> Foundation\Procrun 2.0\protextc\Parameters\Java\
> ```

You must restart Tomcat for this change to take effect on your Protex server.

This system parameter has two settings:

- **False** (Default) - This setting means that the new Suite dashboard is the default landing page when users log in to Protex. Users can still navigate to the classic user interface by selecting **Tools** from the user name menu.
- **True** - This setting means that the Classic dashboard is the default landing page when users log into Protex. Users can still access the new Suite interface by clicking the Protex logo in the header of the Classic interface.

2.11 Allowing Users to Self-Register

You can expose a link on the Protex login screen allowing users to self-register.

When you enable this link, users can navigate to a screen where they can enter their name, email, and a password to create a new user account. The new account is not associated with any projects and does not have roles. The self-registered user is only able to log in and access the Help and documentation links. An administrator must still assign roles and projects.

After these users have registered, you can manage them using the **Tools** area, and assign roles and projects as required.

> **Note:** This setting only controls whether to display the self-registration link.

✱ To show the registration link on the login page:

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Policy Manager**. Protex displays the **Policy Manager General** tab.
4. In the **Registration Link** section, select the **Show Registration Link on Login Page** check box.
5. Click **Save**. This setting takes effect the next time you access the login page.

Chapter 3: Implementing Multi-server Environments

This chapter contains information about configuring a multi-server Protex environment.

The majority of the procedures in this chapter should only need to be performed once, during the initial setup of your Protex environment. However, some procedures are part of routine system maintenance of a multi-server environment.

3.1 Understanding Multiple Server Environments

Protex has two distinct implementations that can involve multiple Protex servers. It is important to understand the difference between these features, and how they are discussed in the Protex documentation.

- **Multi-server Scan** - Designed to distribute the load of scanning and analysis work among more than one server. There is only one complete instance of the Protex server in the deployment; the scan servers have a subset of the Protex software and database, and can only perform analysis work.
- **Multi-server Synchronization** - Designed to synchronize configuration settings and data across multiple Protex server instances. Each Protex server in the deployment has a complete instance of the Protex software and database.

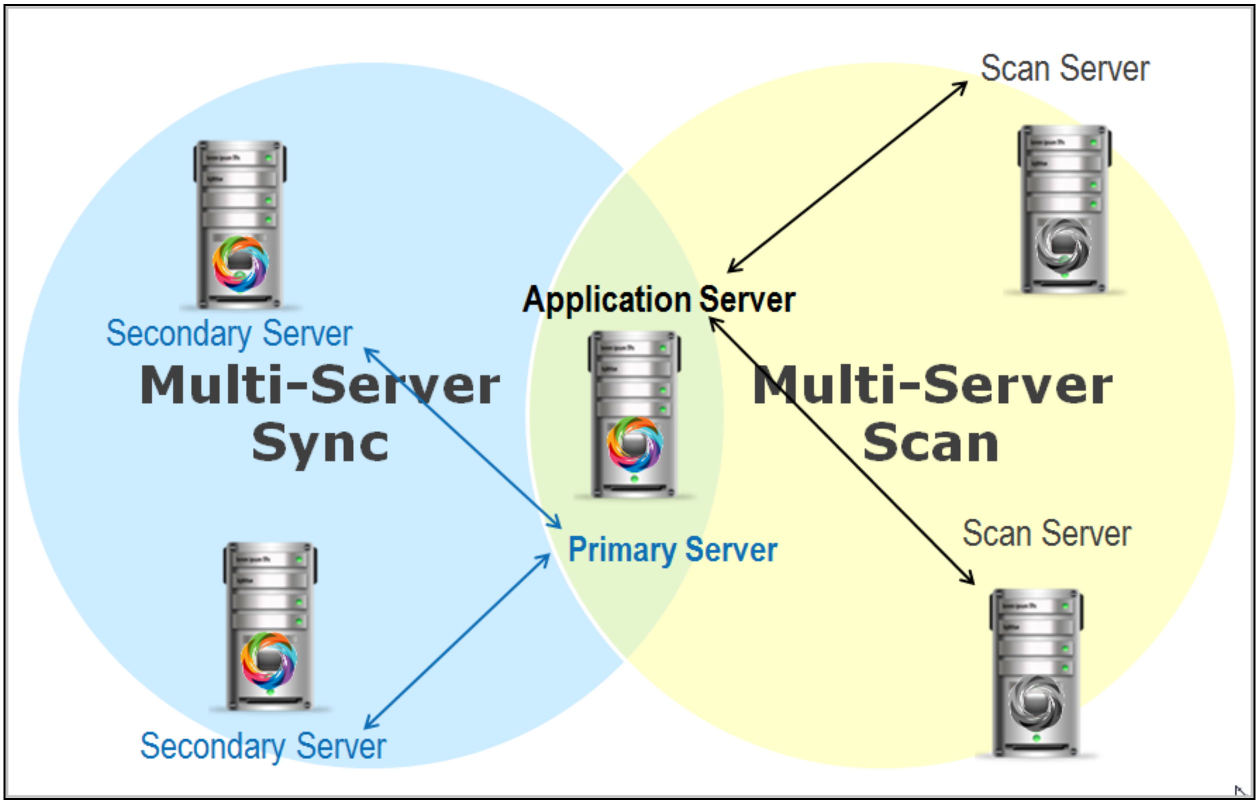
Both of the Protex multi-server environments have one server that is the master for the entire implementation and additional satellite servers.

These two implementations have different purposes and utilize different technologies. To help distinguish between deployments, different terminology is used for the Protex servers, depending on which environment and server is being discussed.

Implementation	Master server	Satellite servers
Multi-server scan	**Application server** - Standard Protex installation.	**Scan server** - No user interface; server can only perform scanning/ analysis work. Available on Linux only.
Multi-server synchronization	**Primary server** - Standard Protex installation.	**Secondary server** - Standard Protex installation with user interface; can be used for all Protex functions. Available on Linux and Windows.

You may choose to implement one or both of these environments. And while they are described separately, it is important to understand where and how the two features intersect.

Figure 3.1: Intersection of the two multi-server Protex environments



If you implemented both environments, the same master Protex server could serve as both the application server and the primary server.

However, because the software deployed on the satellites is different for each environment, a satellite server can be either a scan server or a secondary server, but it cannot be both.

3.2 Understanding a Multi-server Scan Implementation

Note: Protex 7.1 and higher includes access to the multi-server scan feature.

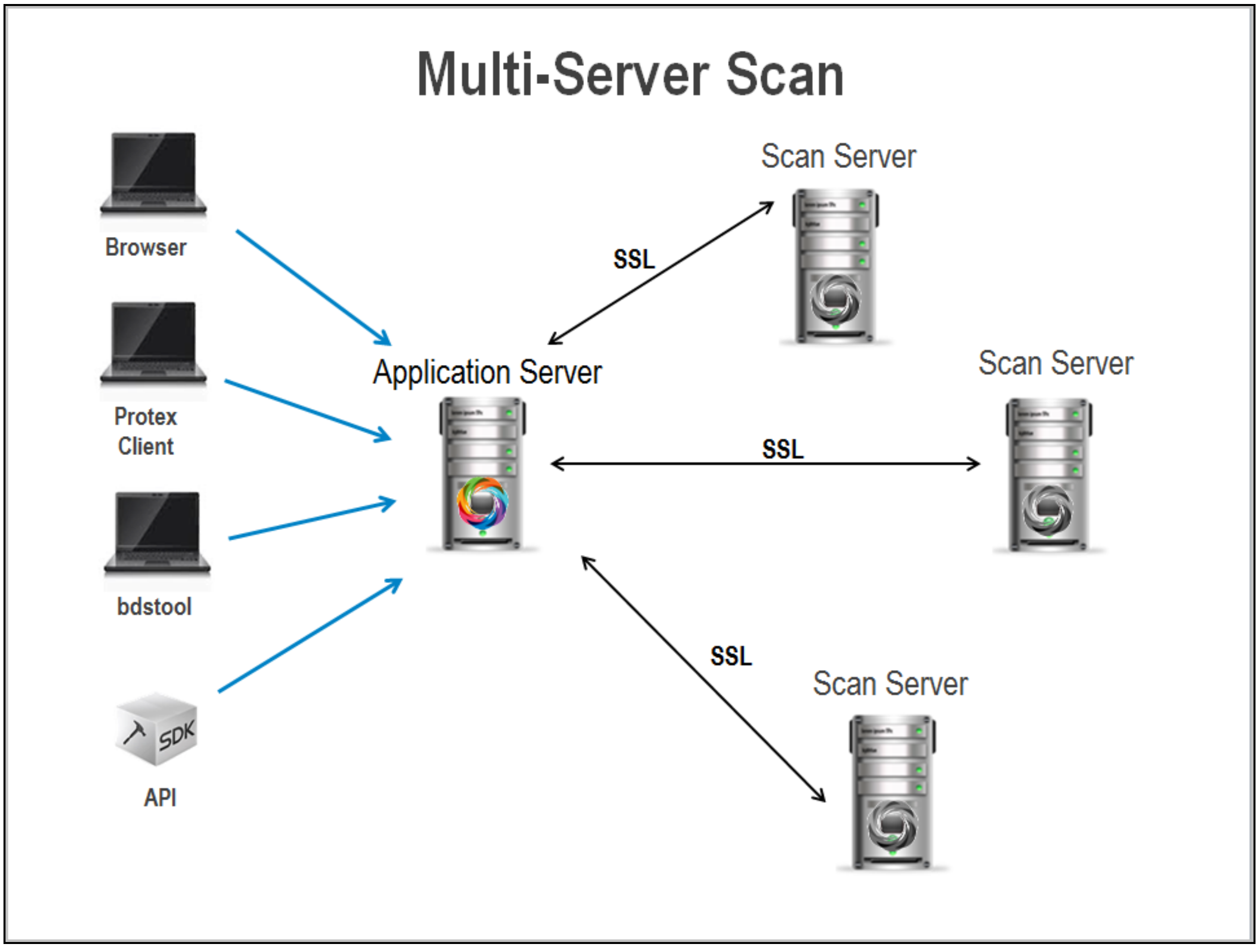
The most resource-intensive part of the Protex workflow is during scanning and analysis, when Protex compares your code to the KnowledgeBase.

Protex 7.1 introduced an early access version of a new multi-server scan feature. This feature provides the option of installing additional (up to two) scan servers, which lets you move the analysis work off your main application server and onto one to two remote scan servers to improve application server UI responsiveness while scanning is performed.

In addition, Black Duck recommends that all Protex servers in your multi-server implementation be co-located with your major source code repositories and build systems; that is, in the same physical location, server room, or rack, to minimize network latency issues during scans.

Note: Protex scan servers are only available for Linux servers. Each scan server requires a separate registration key. The hardware recommendations for scan servers are the same as the recommendations for any Protex implementation.

Figure 3.2: Protex Multi-server Scan implementation



Protex Scan Servers

After installing scan servers, use the **Administration** > **Scans** page to associate them with your main application server. When there is analysis work to be performed, the application server assigns it to the first available scan server. The following components are installed on a scan server:

- **Apache Tomcat** - Tomcat is a web application, a JSP (Java Server Pages) and servlets container. Tomcat provides a environment for Java code to run in cooperation with a web server. It has tools for management and configuration, and can be custom configured using XML-formatted files.
- **PostgreSQL database** - The installer creates the same Protex PostgreSQL databases on the scan server as it creates when installing the application server. The scan server uses the local copy of the KnowledgeBase to improve read performance time while performing analysis. The scan server does not use the local copy of the customer databases; customer data is sent to the application server.

Note: The scan servers do not have a user interface, and cannot be used for Protex tasks other than performing scans and analysis.

For information regarding setting up scan servers as stand-alone servers, refer to the topic *Scan Servers for a stand-alone Protex server Overview* in the *Protex Installation Guide*.

Overview

Databases

Protex utilizes four databases to store KnowledgeBase and customer data. When you install a scan server, the installation program installs the two KnowledgeBase databases (`bds_basic` and `fp_basic`) on the scan server. These local databases are used when the scan server performs analysis work.

The installer also creates the two databases that store customer data (`bds_customer` and `fp_customer`). However, the scan server does not use these two databases to store data. Data created during the analysis phase on the scan server is sent back to the application server for storage in the database on the application server. No analysis data is stored on the scan servers. All customer data is stored on the application server. Because there is no customer data stored on a scan server, you are not required to back up the database on a scan server machine.

The number of scan servers you can implement in a multi-server scan environment is limited to two. This is because scan servers and the application server share the customer databases, and the database connection pool is limited to 200 connection strings.

Caution: Exceeding two scan servers is not supported, because additional scan servers overwhelm the database server's ability to accept connections.

Security

The application server can connect to the scan servers using a standard HTTP or a Secure Socket Layers (SSL) connection.

The scan servers always communicate with the database through SSL. When you enable multi-server scanning, the PostgreSQL database is configured to listen for SSL connections on all addresses. To authenticate, you must make an SSL connection to the database.

Note: If you are not implementing multi-server scan, the installer does not configure PostgreSQL for OpenSSL.

When you add a scan server to your multi-server implementation, the Protex application server creates a signed certificate on the scan server. Scan servers must present a security certificate signed by the application server to access the `bds_customer` and `fp_customer` databases.

Note: A scan server can only be connected to a single application server. An error is generated if the scan server already has a signed certificate for a Protex application server.

The scan servers store their security certificates in the following directory:

```
/opt/blackduck/protexIP/config/pgcert
```

The certificates do not exist when you install the scan server; they are created when you add the scan server to the application server. These certificates should not be altered or deleted by any means other than using the Protex tools.

Source Code

With a multi-scan server environment, the source code must be in a location accessible to the application server, the Protex client, or **bdstool**.

Do not place source code on the scan servers for scanning; the scan servers only perform analysis work.

Analysis

The analysis process consists of four phases:

1. **Initializing** - This is a very brief phase, where Protex reads the configuration settings used for the analysis. If the analysis settings have changed since the last time an analysis was run on the project, Protex displays a dialog box identifying the changed settings. You can choose to run the scan with the changed settings or cancel the scan.
2. **Assessing** - During this phase, Protex counts the files and folders in the project to determine the work to be performed for the scan and analysis. If you are rescanning the project, Protex detects changed files (the delta) based on the settings specified for the project (file modification time or checksums).
3. **Scanning / Code Printing** - During this phase, Protex creates codeprints for the files in the project. A codeprint is an algorithmically generated hash that uniquely identifies a file or code snippet, acting as a digital fingerprint to identify the code. The codeprint files are used to compare the project to the Black Duck KnowledgeBase.
4. **Analysis / Computing the Bill of Materials** - During this phase, Protex compares the codeprints from your project to codeprints for known open source components stored in the KnowledgeBase. After comparing all files, Protex generates the Bill of Materials (BOM) for the project.

In a multi-server scan environment, when you launch a scan (from the Protex application server, the Protex client, or using **bdstool**), the application server no longer performs analysis; instead it acts as a dispatcher, sending work to the scan servers.

The application server pings the scan servers in the deployment on a regular interval, checking each scan server for the following information:

- Protex software version
- KnowledgeBase version
- CPU usage of the scan server
- Number of scan slots available on the scan server

Important: If the scan server is not at the same KnowledgeBase version as the application server, Protex deactivates the scan server and it is unavailable for scans until it is updated to match the application server.

When a scan is initiated, the application server looks for the next available scan server and sends the work to that server. The application server uses a number of different criteria when determining which scan server is assigned each job in the queue, including:

- Time since the scan server was last assigned a scan job.
- Number of scans currently running on the scan server.
- The `blackduck.scan.maxConcurrent` value configured for the scan server, or a reasonable default if set to unlimited.
- Maximum heap space available to the server.
- Number of CPUs available to the Java virtual machine.
- Reported CPU load on the server.

All scanning is performed on the scan servers. The only time that scanning work is performed on the application server is if the scan servers are offline or need updating.

Logging

All logging for a multi-server scan environment happens on the application server in the Black Duck log file, which is located at:

```
/opt/blackduck/protexIP/tomcat/logs/blackduck_log.txt.<date>
```

Upgrading

Before upgrading your system, stop any scans running on the deployment.

1. Upgrade the application server, either manually or on an automatic schedule. While the application server is updating, it is not sending work to the scan servers.
2. The application server pings the scan servers, verifies that the software or KnowledgeBase version does not match the version of the application server, and marks each of the scan servers as *Needs Update*.
3. If scans are triggered before the scan servers are upgraded, these scans are processed by the application server.
4. The application server initiates the upgrade of the scan servers, one at a time. As the update completes for each scan server, its status returns to *Online* and it is available for work assignments from the application server.

The only downtime during upgrades is while the application server itself is upgrading.

3.3 Understanding Placeholders

Black Duck does not require that all servers be at the same KnowledgeBase level; therefore, *placeholders* are utilized. Placeholders are defined as a temporary representation of Black Duck KnowledgeBase data for use until a KnowledgeBase update with that data is received.

If your servers are out-of-sync with KnowledgeBase versions, placeholders are created which contain the same license and data as the license in the KnowledgeBase on that system. When KnowledgeBase versions do not match, placeholders are only used to reference an item that is missing due to differing KnowledgeBase versions; for example, a component license. If you are using a new standard reference library, then placeholders are not used.

You cannot edit or modify placeholders. After a KnowledgeBase update occurs and both servers have the same KnowledgeBase version, the placeholder is automatically replaced by the KnowledgeBase data.

Note that codeprints are automatically copied over. Multiple licenses and standard components are synchronized. A component can reference a license when used at the policy level. A component cannot be used at the policy level. Placeholders are only used if the component is modified.

Custom Component Versioning: Custom Component Versions (CCVs) are synchronized with actual codeprints to be the same across servers, regardless of file/directory location. Source files and analysis source file paths are not synchronized. However, you can manually synchronize using the **Add component to BOM** functionality.

If the component existed on both servers, then the analysis source location remains unaltered on both servers. The source location defaults to blank on the destination server. The source location may show as blank if the CCV has not been codeprinted, or if the CCV has been synchronized but never previously existed on that server.

In Code Center, a placeholder is seen as a custom component.

Protex/Code Center synchronization does not synchronize Bills of Materials; it synchronizes components, licenses, and obligations. If project-related data synchronization between Protex servers is in use, you cannot enable Code Center/Protex synchronization which synchronizes components, licenses, and obligations between the Code Center and Protex servers. You can still use import and validate functionality with Code Center in this Code Center/Protex environment scenario. If you have a placeholder component in your Protex Bill of Materials, and perform an import or validation with Code Center, the component is seen as a custom component in Code Center.

For more last-codeprinted information within Protex, refer to **Details** > **Source Location**.

3.4 Implementing a Multi-Server Scan Environment

The multi-server scan environment requires SSL. Only the Protex-supported Linux operating systems are supported for multi-server scan environments.

> **Note:** The multi-server scan environment is not available for Windows.

> **Note:** The **Administration** page for the multi-server scan environment is only available in the Suite interface. If you have disabled the Suite interface, you cannot create or manage scan servers.

There are no additional port requirements. The database port on the application server (55432 by default) must be open to traffic from the scan servers. It only accepts SSL connections.

New Protex Implementation

If you are implementing a multi-server scan environment for a new Protex implementation, the steps are:

1. On the machine to host the application server, install the full Protex server from the installation media.
2. On the machines to use as scan servers, perform a scan server installation from the installation

media.

3. Log into the application server as an administrator.
4. Add the scan servers. For more information, refer to Adding a Scan Server on page 46.

Note: If you are using LDAP, you must copy your `config/custom.properties` file from the application server to each of your scan servers. You must restart Tomcat on the scan server for the configuration changes to take effect.

Important: A stand-alone server can only be converted to an application server, not a scan server. Scan servers must be installed on a fresh system.

3.4.1 Operating System Requirements - Protex scan server

You must be on one of the supported 64-bit operating systems to have the minimum version of Open SSL supporting a scan server environment. For a complete listing of the platforms that are tested and supported for this release, refer to Supported Operating Systems.

Note: Windows operating systems are not supported with Protex scan servers.

3.4.2 Configuring the Maximum Number of Concurrent Scans

Protex has a system property for the maximum number of scans that can be run at the same time. This property applies to all Protex servers; you can configure it even if you do not have a multi-server scan implementation. The system property is:

```
blackduck.scan.maxConcurrent
```

A negative value does not limit the number of scans. The default value is set to `-1`, which indicates no limits on the number of scans. A positive value limits the number of scans that can be run simultaneously by the servers, including the scans running on scan servers in a multi-server scan environment.

Note: This property does not control the scans triggered by integration plug-ins; for example, the Jenkins plug-in, or by scans triggered by the **bdstool** command line utility. Thus, it is possible to run more scans concurrently than the value specified in this system property.

In a multi-server scan environment, you can set this value on both the application server (to control the total number of scans), and on the scan servers (to control the maximum number of scans on that server instance). For example, if you have a multi-server scan environment with two scan servers, where one server is less powerful than the other, you can set the maximum number of scans for deployment on the application server, and you could limit the number of scans that can be assigned to the less-powerful server.

✱ To configure the maximum number of scans:

1. On your server, navigate to the Tomcat startup file:

```
/opt/blackduck/protexIP/config/bds-protexIP-tomcat.start
```

2. Open the file with a text editor.
3. Add the following to the end of the file to specify the maximum number of scans that Protex should run at one time:

   ```
   export JAVA_OPTS=" -Dblackduck.scan.maxConcurrent=<value> ${JAVA_OPTS}"
   ```

   A positive number limits the number of scans. A negative value does not limit the number of scans. The default value is `-1` (no limit).
4. Save the file.
5. Restart Tomcat on the server.

3.4.3 Adding a Scan Server

After installing a scan server, you must associate it with the application server. You can associate a scan server with the application server from the **Administration** page on the application server.

You must be on one of the following operating systems to have the minimum version of Open SSL supporting a scan server environment:

Operating System	Version
Red Hat® Enterprise Linux® Server	6.4, 6.5, 7.0, and 7.1 for 64 bit AMD64/Intel EM64T
Oracle® Linux®	6.4, 7.0, and 7.1
Novell SUSE® Linux®	10.1 (x86_64)
SUSE® Linux® Enterprise Server	10, 11, 12 (x86_64)
CentOS	6.5, 6.6, 7.0

Note: Note that when you add a scan server to your multi-server scan deployment, you do not need to restart either the database or Tomcat.

✱ To add a scan server:

1. Log in to the application server as an administrator.
2. From the user name menu in the **Suite** interface, select **Administration**.
3. Click the **Scans** tab.
4. Click **+ Add Scan Server**.
5. In the **Add Scan Server** dialog, enter the **Scan Server URL** for the application server to use for connect ing to the new scan server; for example:

   ```
   http://scanserver01.example.com/
   ```

   or:

   ```
   https://scanserver02.example.com/
   ```

2. Enter the **Scan Server Name**; for example, *scanserver1*.
3. Click **Create**.
4. Protex displays a message asking if you want to trust the scan server. To grant the scan server access to the database, click **OK**.
5. If the scan server is installed but the scan server license has not yet been registered, Protex displays a prompt to enter the license key and complete the registration.

Protex adds the server to the **Administration** > **Scans** page and displays its status.

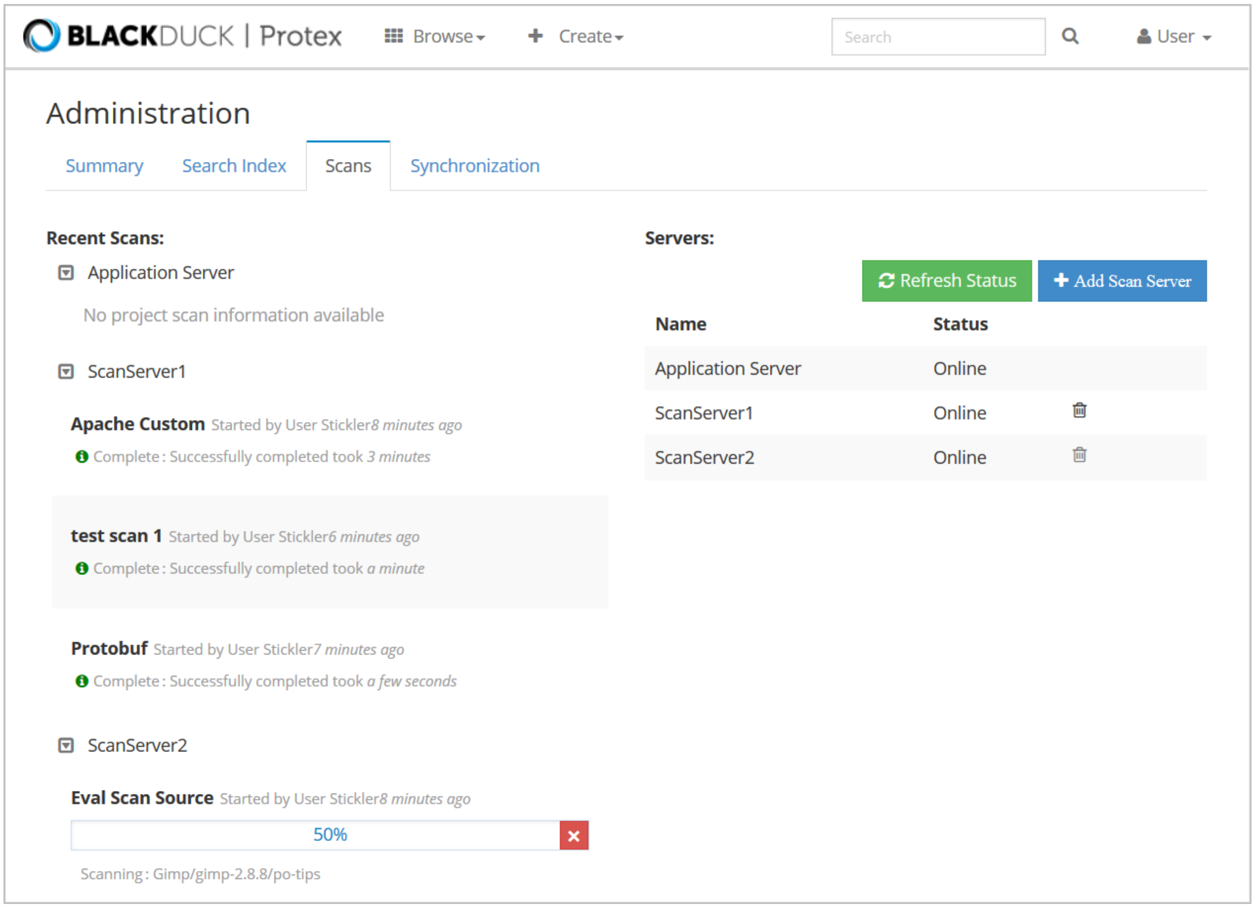
3.4.4 Viewing Scan Server Status

If you have the administrator role, you can view all scans currently running on your Protex deployment using the **Administration** > **Scans** page in the Suite interface.

This page displays all scans, including scans initiated either locally or remotely from the following sources:

- Scans initiated from the user interface through a browser.
- Scans initiated from the Protex client.
- Scans initiated by the **bdstool** command line tool.
- Scans initiated by an integration plugin; for example, the Protex Jenkins plug-in.
- Scans initiated using the Protex API.
- Scans initiated remotely from multiple sources; for example, scans initiated remotely from the Protex SDK, **bdstool**, Protex UI client, or Protex integration plugin products.

Figure 3.3: **Administration** > **Scans** page showing recent scans and server status



Administration

Recent Scans:

Application Server

No project scan information available

ScanServer1

Apache Custom Started by User Stickler8 *minutes ago*

Complete : Successfully completed took *3 minutes*

test scan 1 Started by User Stickler6 *minutes ago*

Complete : Successfully completed took *a minute*

Protobuf Started by User Stickler7 *minutes ago*

Complete : Successfully completed took *a few seconds*

ScanServer2

Eval Scan Source Started by User Stickler8 *minutes ago*

50%

Scanning : Gimp/gimp-2.8.8/po-tips

Servers:

Name	Status
Application Server	Online
ScanServer1	Online
ScanServer2	Online

The **Administration** > **Scans** page displays the following information about your multi-server scan implementation:

- Currently running scans, including the scan status, a stop scan button, and which scan server is processing the scan.
- Recent scans, including the scan duration, and which scan server processed the scan.
- Names of all servers in the multi-server implementation.

Tip: To view the scan server URL, hover over the name of the server.

- Status of each server.

A server in a multi-server implementation can have one of the following statuses:

- **Offline** - Indicates that the application server cannot communicate with the scan server; for example, if the network is down.
- **Online** - Indicates that the server is available to perform work. This indicates that the scan server is at the same update level as the application server, and the application server can communicate with the scan server.
- **Refreshing** - Indicates that Protex is actively loading the latest status from the scan server.

- **Requires Manual Upgrade** - Indicates that the application server is unable to automatically upgrade the scan server and the upgrade must be performed manually.
- **Requires Upgrade** - Indicates that the last time the application server communicated with the scan server, either the software or the KnowledgeBase version on the scan server did not match the version on the application server. The application server changes the status of the scan server to **Requires Upgrade**, and automatically triggers the upgrade on the scan server.
- **Unrecoverable** - Indicates that the scan server either no longer has a valid registration key, or that it has lost its signed certificate.
- **Upgrading** - Indicates that the server is in the process of upgrading; either a software upgrade or a KnowledgeBase update.

3.4.5 Refreshing Scan Server Status

Click **Refresh Status** to force the application server to communicate with each of the scan servers and refresh the statuses displayed on the **Administration** > **Scans** page. The Protex application server communicates regularly with the scan servers, but you can use this option to force communication with the scan servers.

✱ To refresh server status for all servers:

1. Log in to the application server as an administrator.
2. From the user name menu in the **Suite** interface, select **Administration**.
3. Click the **Scans** tab.
4. Click **Refresh Status**.

3.4.6 Renaming a Scan Server

You can rename a Protex scan server. This might be advantageous when reconfiguring your server environment or adding servers, causing the need for a new naming convention.

> **Note:** To change the host name of a scan server, you cannot edit the name; you must remove the scan server and re-add it with the new name.

✱ To rename a Protex scan server:

1. Remove the scan server you want to rename from your multi-server implementation. Refer to Removing a Scan Server on page 49.
2. Rename the server.
3. Add the server back into your multi-server implementation. Refer to Adding a Scan Server on page 46.

3.4.7 Removing a Scan Server

You may want to remove a scan server from your multi-server implementation because you want to take the server offline, remove an offline server from the configuration, or rename the server.

Note: If the scan server is online when you remove it, this action removes the security certificate from the scan server. If the scan server is offline when you remove it, the security certificate cannot be removed and the server cannot be assigned to another application server. Contact Black Duck Support for help.

To remove a scan server:

1. Log in to the application server as an administrator.
2. From the user name menu in the **Suite** interface, select **Administration**.
3. On the **Administration** page, click the **Scans** tab.
4. In the **Servers** column on the **Scans** page, next to the server to delete, click the **Delete** icon (🗑) .
5. In the **Delete Server Confirmation** dialog box, click **Confirm**.

3.4.8 Troubleshooting a Multi-Server Scan Environment

Logging

All logging for a multi-server scan environment occurs on the application server in the Black Duck log file. The path for the log file is:

```
/opt/blackduck/protexIP/tomcat/logs/blackduck_log.txt.<date>
```

Scan Failures

If you are using LDAP for user authentication, you must also configure your scan servers for LDAP. To do this, copy the `config/custom.properties` file from the application server to each of your scan servers. You must restart Tomcat on the scan server for the configuration changes to take effect.

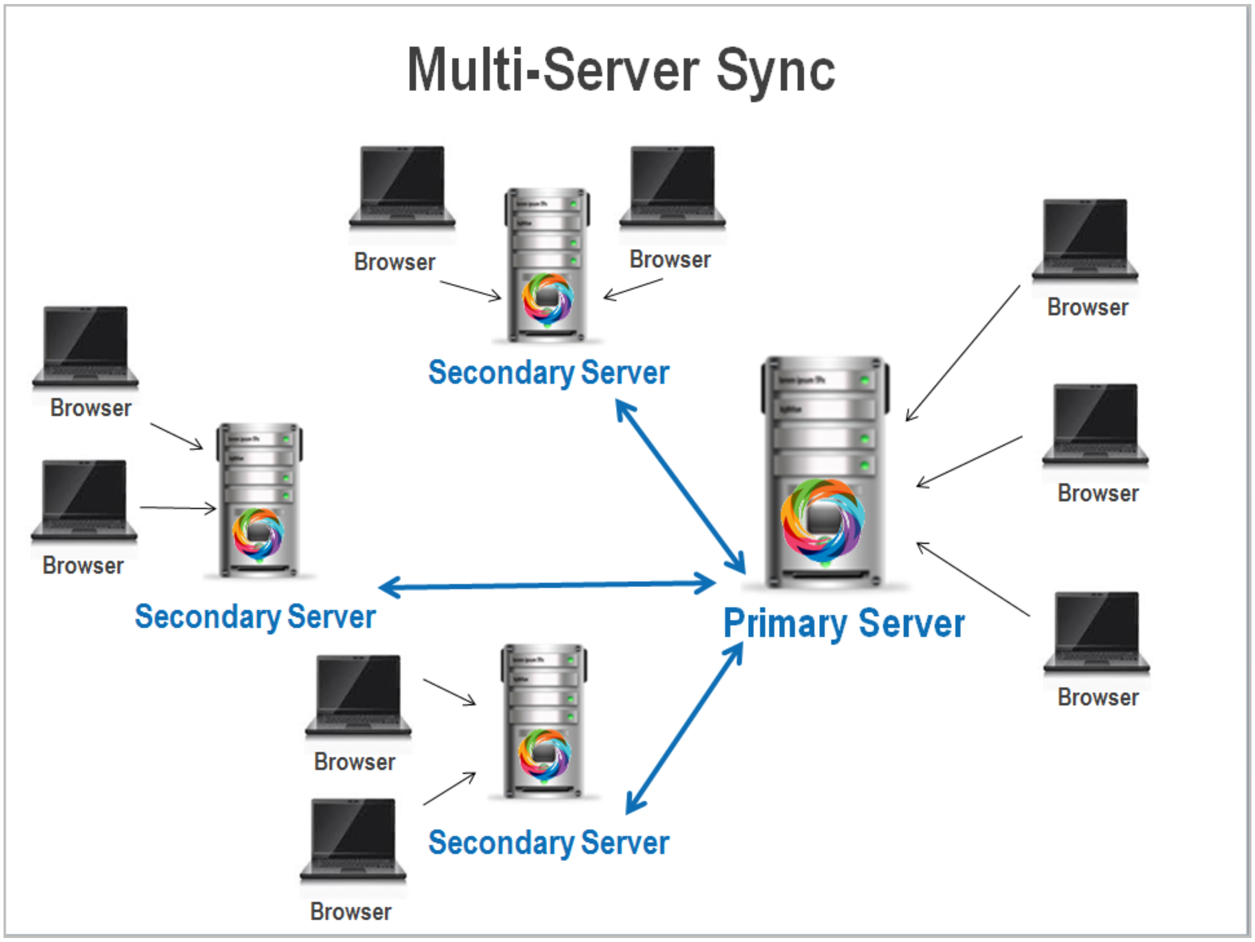
Unrecoverable Scan Server Status

The *Unrecoverable* status for a scan server indicates that the scan server has either lost its signed certificate, or no longer has a valid registration key. If you have a server with an *Unrecoverable* status, remove the server and then re-add it. Removing and re-adding the server should repair most certificate problems. If there is a problem with the registration key, Protex displays a dialog box to re-enter your registration key. For more information, refer to Removing a Scan Server on page 49 and Adding a Scan Server on page 46.

3.5 Understanding Multi-Server Synchronization Implementation

The multi-server synchronization feature provides a way to synchronize configuration settings and data across multiple Protex server instances. Designate one Protex server as the primary server, and then associate one or more secondary servers with the primary server. There is no practical limit to the number of secondary servers you can add to your Protex environment.

Figure 3.4: Protex Multi-server Synchronization implementation



Protex Synchronization Servers

Each server in a multi-server synchronization deployment is a full installation of the Protex software and databases.

Define the primary Protex server when you associate a secondary server with one of your Protex servers. There can be only one primary Protex server per deployment, but there can be one or more (no practical limit) secondary Protex servers.

The settings and data that are synchronized can be configured separately for each secondary server. For example, one server might be configured to synchronize all possible settings and data with the primary server, while another might synchronize only global discovery and identification options.

Synchronization

Data synchronization occurs automatically in real-time; data added or changed is immediately synchronized across all severs in your multi-server synchronization environment. The multi-server synchronization feature uses a Java Messaging System (JMS) to send information back and forth between servers in the environment. The exchange of information through the messaging service is bi-directional; that is, both the primary and secondary servers send data to each other. Data stored on the primary server is downloaded to the secondary servers, and data stored on the secondary servers is uploaded to the primary server.

When you have implemented multi-server synchronization, Protex performs two different types of synchronization:

- **Full synchronization** - Occurs when Protex performs the initial synchronization when you add a secondary server. In a full synchronization, when there are conflicts between data being synchronized on the primary and a secondary server, the data on the primary server takes precedence. The synchronized data on the secondary server is overwritten with the data from the primary server.

After the initial sync, the primary and secondary servers communicate using the JMS message service. For more information, refer to Configuring JMS Communications for Multi-Server Synchronization on page 56.

Note: You can also force a full synchronization from the primary or secondary server in your multi-server synchronization deployment.

- **Incremental synchronization** - Occurs after the initial synchronization between the primary and secondary servers. As changes are made on servers in the deployment, Protex updates the other servers in the deployment. Changes on the secondary servers are uploaded to the primary server and then propagated to the other secondary servers. Changes on the primary server are also sent to the secondary servers.

Data Updates

How incremental synchronization updates work:

- If there have been multiple concurrent changes to the same data on different servers, Protex keeps the most recent update.
- If the primary server cannot reach a secondary server; for example, if the network connection is lost, the primary server attempts to synchronize again at the next scheduled interval.
- When a secondary server cannot be contacted during an update, the primary server retries communication at a user-configurable interval until communication is re-established or until the server is manually removed from the list of secondary servers.
- Before and after values for all updates are written to the log files at the default logging level (INFO).
- If Protex fails to update a secondary server, it is logged as an error on the primary server. This could occur when the primary server cannot communicate with the secondary server.
- If Protex fails to apply data changes on a secondary server, it is logged as an error on the secondary server. This could occur if there are data integrity problems, in which case Protex attempts to correct the problem.

User Permissions

In a standard Protex implementation, a user's ability to view, create, and modify data is controlled by their user roles.

In a multi-server synchronization implementation, a user's ability to view, create, and modify data is controlled by the normal user roles, but in addition, the server synchronization role is required. The only permission granted by this role is the ability to edit data that is synchronized with other Protex servers. Enabling multi-server synchronization locks settings and data for users that do not also have the additional server synchronization role.

Source Code and Analysis

Within a multi-server synchronization implementation, source code available to a Protex server can be scanned and analyzed by that server instance. You can synchronize some of the global policies and settings determining how Protex performs analysis. Projects and access to source code is not shared or synchronized between servers. Scanning and analysis are performed separately on each individual Protex server.

Logging

There is a new synchronization log (`synchronization_log`) on each server in a multi-server synchronization environment. These logs are visible on the **Tools** > **Admin Center** > **View Logs** page in the classic interface.

Protex logs before and after values for all synchronization updates, and these values are logged at the default logging level (INFO).

Failure to update data on a secondary server is logged as an error in the logs on the primary server.

Failure to apply data changes on a secondary server are logged as an error in the logs on the secondary server.

Upgrading

In a multi-server synchronization environment, the primary server should always have the most current Protex software version and the latest KnowledgeBase data. When you implement the multi-server synchronization feature, configure your scheduled updates so that the primary server updates or upgrades before the secondary servers.

Data Synchronization Recovery Mechanisms

Because the multi-server synchronization environment is network-dependent, there may be instances wherein the network is down or other network communication issues occur. Data synchronization for multi-server synchronization environments occurs automatically and in real-time. However, should network issues arise, you can depend on two recovery mechanisms:

- **Forced synchronization**: On the **Synchronization** tab, click **Synchronize**. This forces an immediate multi-server synchronization.
- **One-week synchronization**: Once per week, Protex executes a multi-server synchronization. This functions like a backup operation, synchronizing all data across your entire multi-server synchronization environment. If data was not synchronized due to network issues, the automatic weekly synchronization ensures that no data is lost; nor are servers ever out of synchronization. The once-weekly time period is the default; you can change the time period or disable this feature. For more information, refer to Configuring JMS Communications for Multi-Server Synchronization on page 56.

3.5.1 Multi-Server Data Synchronization in 7.4 and higher

When adding or editing a secondary Protex server running version 7.4 or higher, additional data synchronization categories automatically display.

The Protex multi-server synchronization feature allows you to select data options from the following list for synchronizing between the primary server and one or more secondary servers. For more information, refer to Adding a Secondary Server for Synchronization on page 63.

The categories which automatically display when adding or editing a Protex server running version 7.4 or higher are:

- Users
  - Users
  - User Roles
- Policies
  - Code Label Policies
  - Analysis Database Policies
  - Access Policies
  - Source Handling Policies
  - Identification Policies
  - Match Retention Policies
  - Match Detection Policies
- File Patterns
  - File Patterns
- Project Related Data
  - Obligation Categories
  - Obligations
  - Licenses
  - Components
  - String Searches
  - Code Prints
- Report Templates
  - Report Templates
  - Report Template Options
- Learned Identifications
  - Learned String Search Identifications
  - Learned Code Match Identifications

- Learned Declared Identifications

3.6 Implementing Multi-Server Synchronization

If you have multiple Protex servers that you want to configure to work together in a Multi-Server Synchronization environment, the general steps are as follows.

> **Note:** Your Protex servers must be upgraded to at least Protex 7.1 before you can implement multi-server synchronization.

Step 1 - Plan what data you want to synchronize

Before you implement Multi-server Synchronization, you should read Data That Can Be Synchronized and determine what data you want to synchronize between servers. Note that you can configure what settings and data are synchronized separately for each secondary server.

Step 2 - Identify the primary server

Identify which server you want to be your primary server. The primary server is responsible for managing the network of synchronized servers and resolving data conflicts when they occur. In the initial synchronization with a new secondary server, if there are data conflicts between data on the primary server and secondary servers, the data on the primary server wins. That is, the system automatically defaults to the data on the primary server when performing a complete sync from the primary server.

When selecting which Protex server will be your primary server, select the one that whose data and global settings are what you want to propagate across the rest of your Protex servers. You may need to modify the data on your primary server to match what you intend to synchronize across all servers. For example, if a user has the Project Leader role on the primary server, but has the Administrator role in a secondary server, you will want to grant them the Administrator role on the primary server to you do not overwrite their permissions during the initial synchronization.

Step 3 - Grant the Synchronization role to users

Once you have selected data or configuration settings for synchronization, that data can only be modified by users who have the Synchronization role as part of their user profile. The only permission granted by this role is the ability to modify data that is being synchronized between servers. Users must be assigned additional roles beyond the Synchronization role in order to perform work.

Before you begin your implementation, grant the synchronization user role to any users who will be allowed to modify synchronized data. These users might include any of the following:

- Uses with the System Administrator role on the primary server
- Uses with the System Administrator role on the secondary servers
- Other users on the primary server
- Other users on the secondary servers

Step 3 - Add Secondary Servers

Once you have determined what settings and data you will synchronize, you can Add a Secondary Server for Synchronization.

3.6.1 Configuring JMS Communications for Multi-Server Synchronization

The multi-server synchronization feature uses a Java Messaging System (JMS) to send information back and forth between the servers in the environment. JMS is a messaging standard that allows application components based on the Java Enterprise Edition (Java EE) to create, send, receive, and read messages. Protex uses the ActiveMQ (Apache) implementation of JMS which uses the Java Authentication and Authorization Service (JAAS). JAAS is an industry-standard security framework.

JMS communications happen over the same HTTP port used by Protex. You do not need to open additional ports if you enable a multi-server synchronization environment. If you configure HTTPS (SSL) for your Protex implementation, the messaging service also uses HTTPS.

> **Note:** If you are implementing HTTPS with a multi-server sync implementation, you should use a method that allows communication between servers without providing a password; for example, public-private keys.

The Protex JMS messaging provider is exposed as a servlet of the main application, under the following context path:

```
<Protex URL>/messaging/activemq
For example: http://YourServer:8443/messaging/activemq
```

By default, the Protex JMS provider does not perform authentication. If you do not want to perform authentication, no additional configuration is required for the Java Messaging System to work.

However, if you want your Protex JMS provider to perform authentication, the configuration is a two step process:

1. Configure authentication for the JMS provider. Perform this configuration on the primary server in your multi-server synchronization implementation.
2. Configure the servers with credentials to talk to the provider. You must perform this configuration on each server (primary and all secondary servers) in your multi-server synchronization implementation.

Configuring authentication for the Java Messaging System provider

If you want your Protex JMS provider to perform JAAS authentication, you must configure the following options on your primary server:

- blackduck.activemq.group.admin
- blackduck.activemq.group.user
- java.security.auth.login.config

The options are described in the following table, and instructions for configuring these options are given at the end of this topic.

Configuring the credentials to talk to the Java Messaging System provider

If you have decided to enable JAAS authentication on your Protex JMS provider, you must also specify the credentials to talk to the provider. Protex uses a standard callback pattern to read the name and password used to access the JMS server. A callback is a Java class which implements an interface called `CallbackHandler`. You can configure the callback handler Protex uses with the `blackduck.synchronization.jms.callback` system property. You can use the provided callback handler, or write your own, add it to the Protex classpath, and set the system property to use the custom callback handler. Note that any custom callback handlers must support inputs for `NameCallback` and `PasswordCallback`, and the values returned must be valid credentials as configured for the Protex JMS provider.

The following table lists the configurable options (controlled through the system properties) for the Protex embedded JMS provider. For more information about Java authentication and authorization services (JAAS), refer to the Oracle documentation.
http://docs.oracle.com/javase/7/docs/technotes/guides/security/jgss/tutorials/LoginConfigFile.html

Property	Default	Use
`blackduck.activemq.group.admin`	null	A comma-separated values list of Java authentication and authorization service (JAAS) names of principals (groups) of users which are allowed to perform administrative operations on the JMS provider. (Create queues/topics.)
`blackduck.activemq.group.user`	null	A comma-separated values list of JAAS names of principals (groups) of users which are allowed to perform read and write operations on the JMS provider. (Send and receive messages.)
`blackduck.homeURL`	null	This is a pre-existing Protex property that stores the location of the Protex installation directory. This property is used as a base directory to find default configuration files and storage locations for message persistence records. This property is set during installation.

Property	Default	Use
blackduck.messaging.clearPersistenceRecords	null	This option should only be used if your system is down and you need to recover from a completely corrupt message persistence store. If you have gotten into a state where your message store is corrupted and unrecoverable, you can set this option to `true` for the system to automatically delete the existing persistence records before attempting to start, allowing a clean re-initialization. **Caution: All messages stored in the existing store are deleted. The store files are cleared every time the system starts when this option is `true`. If this option is used, users should immediately remove it from their options after the system starts.**
blackduck.messaging.durable.expire.hours	8	The number of hours persistent messages should be kept before being discarded. In the context of synchronization, message persistence allows secondary servers that have lost connection to receive messages they missed. The longer the persistence time, the less likely a server is to miss a message, causing a longer operation required to fix the problem. However, longer persistence times cause larger persistence storage files.
blackduck.sync.recurring.import.frequency	10080	The number of minutes between a recurring full import process. The default is seven days. Setting the property to 0 disables this feature. You can configure the synchronization network to automatically perform a full synchronization to keep data consistent across servers despite network connection issues. The full synchronization process attempts to repair connection issues.
blackduck.synchronization.jms.callback		The fully qualified Java class name of a class on the classpath of Protex which implements `javax.security.auth.callback.CallbackHandler` and handles inputs of type `javax.security.auth.callback.NameCallback` and

Property	Default	Use
		`javax.security.auth.callback.PasswordCallback` in a way which returns valid credentials for the JMS provider. **Note:** You must configure Protex to use the default callback handler.
`java.security.auth.login.config`	null	A Java standard property used with the Java Authentication and Authorization Service (JAAS). This property can be used in conjunction with the group properties to configure custom authentication. This property indicates the location of a JAAS configuration file whose setup is dictated by the standard JAAS framework.

If you use the callback handler provided with Protex (`com.blackducksoftware.suite.synchronization.callback.PropertyCallbackHandler`) you must also specify the following property values required by the default handler:

Property	Value
`blackduck.synchronization.jms.propertycallback.user`	The user name for accessing the JMS provider.
`blackduck.synchronization.jms.propertycallback.password`	The password for accessing the JMS provider in Base64 encoding.

✱ **For Linux: To configure system properties for the JMS server, complete the following steps on each Linux server in your multi-server synchronization environment:**

1. On your server, navigate to the Tomcat startup file.

   `/opt/blackduck/protexIP/config/bds-protexIP-tomcat.start`

2. Open the file with a text editor.

3. Add the configuration options to the end of the startup file to specify the properties you want to configure.

   a. Configure your primary server to enable JAAS authentication. For example:

```
export JAVA_OPTS=" -Dblackduck.activemq.group.admin=group1, group2
${JAVA_OPTS}"

export JAVA_OPTS=" -Dblackduck.activemq.group.user=user1, user2, user3
${JAVA_OPTS}"

export JAVA_OPTS=" -
Djava.security.auth.login.config=file:///opt/blackduck/protexIP/config/jm
s-login.config ${JAVA_OPTS}"
```

4. If you have configured your primary server to enable authentication, you must also configure all your servers (primary and all secondary servers) to specify the callback handler providing credentials, and the values for `NameCallback` and `PasswordCallback`. For example:

   ```
   -
   Dblackduck.synchronization.jms.callback=com.blackducksoft
   ware.-
   suite.synchronization.callback.PropertyCallbackHandler

   -
   Dblackduck.synchronization.jms.propertycallback.user=<use
   r>

   -
   Dblackduck.synchronization.jms.propertycallback.password=
   <Base64 encodedpassword>
   ```

5. Save the file.
6. Restart Tomcat on the server.
7. Repeat the steps on each Linux server in your multi-server synchronization environment.

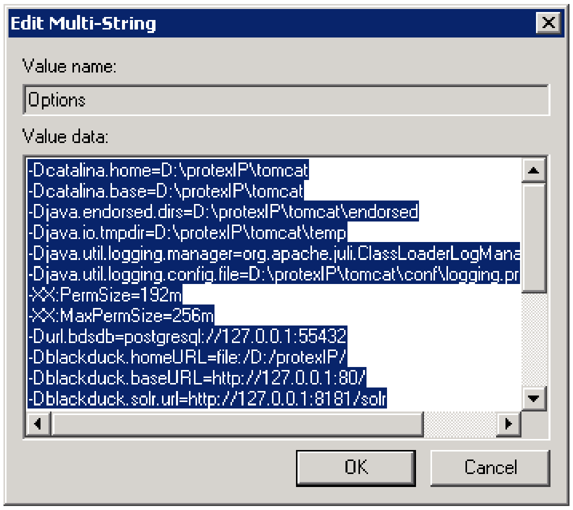
✱ **For Windows: To configure system properties for the JMS server, complete the following steps on each Windows server in your multi-server synchronization environment:**

1. On your server, navigate to the Windows Registry by clicking **Start** > **Run**, and in the **Run** box, type `regedit`. Press Enter, and the **Registry Editor** opens.
2. The Tomcat startup settings are configured in the following Windows Registry key. In the **Registry Editor**, navigate to:
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\protextc\Parameters\Java\`
3. Double-click the **Data** value for this registry key. The **Edit Multi-String** dialog opens.
4. From the following list, select the values pertaining to your environment:

   ```
   -Dcatalina.home=D:\protexIP\tomcat
   -Dcatalina.base=D:\protexIP\tomcat
   -Djava.endorsed.dirs=D:\protexIP\tomcat\endorsed
   -Djava.io.tmpdir=D:\protexIP\tomcat\temp
   -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
   -
   Djava.util.logging.config.file=D:\protexIP\tomcat\conf\logging.prop
   erties
   -XX:PermSize=192m
   -XX:MaxPermSize=256m
   -Durl.bdsdb=postgresql://127.0.0.1:55432
   ```

```
-Dblackduck.homeURL=file:/D:/protexIP/

-Dblackduck.baseURL=http://127.0.0.1:80/

-Dblackduck.solr.url=http://127.0.0.1:8181/solr

-Dblackduck.solr.data.dir=D:\BDS-ProtexIP\solr

-Dblackduck.fingerprintfile.rawfp_dir=D:\BDS-ProtexIP\bds-data

-Dorg.apache.cxf.Logger=org.apache.cxf.common.logging.Log4jLogger

-
Dorg.restlet.engine.loggerFacadeClass=org.restlet.ext.slf4j.Slf4jLo
ggerFacade

-Dfile.encoding=UTF-8

-Duser.country=

-Duser.language=en

-Dblackduck.defaultUpdateLevel=130

-Duser.variant=
```

5. Copy the selected values, and paste them into the **Value data** text box in the **Edit Multi-String** dialog. Note that each value must be on its own line. The following example shows more values than are typically used; this is only for illustrative purposes.



Value name:

Options

Value data:

```
-Dcatalina.home=D:\protexIP\tomcat
-Dcatalina.base=D:\protexIP\tomcat
-Djava.endorsed.dirs=D:\protexIP\tomcat\endorsed
-Djava.io.tmpdir=D:\protexIP\tomcat\temp
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogMana
-Djava.util.logging.config.file=D:\protexIP\tomcat\conf\logging.pr
-XX:PermSize=192m
-XX:MaxPermSize=256m
-Durl.bdsdb=postgresql://127.0.0.1:55432
-Dblackduck.homeURL=file:/D:/protexIP/
-Dblackduck.baseURL=http://127.0.0.1:80/
-Dblackduck.solr.url=http://127.0.0.1:8181/solr
```

6. Click **OK**.
7. Restart the server.
8. Repeat this process for each Windows server in your multi-server synchronization environment.

3.6.2 Configuring Multi-server Synchronization URLs

The messaging service used by multi-server synchronization to communicate between servers requires an externally reachable URL for each server in the environment.

The messaging service initially loads the Protex system property `blackduck.baseURL`. If the `blackduck.baseURL` property for the primary server is set to `localhost`, Protex requires that you configure an externally reachable URL for the primary server before you can add secondary servers to the configuration.

Specify an externally reachable URL for the secondary server when adding secondary servers.

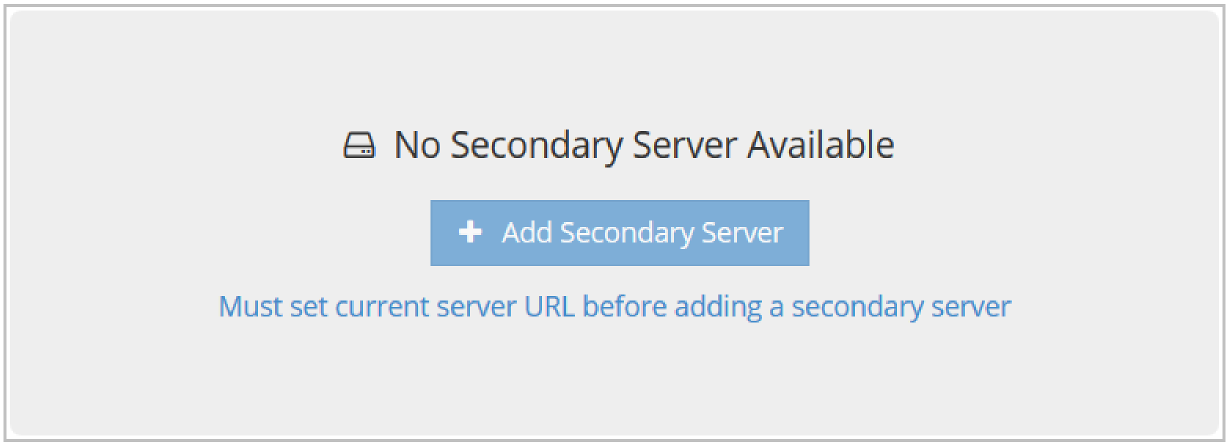
To configure multi-server synchronization URLs, the following user roles are required:

- A user account with the administrator role and the server synchronization role on the primary server.
- A user account with the administrator role on the secondary server.

To configure the URL for the primary server:

1. Log in to the primary Protex server as a user with the administrator role.
2. From the user name menu in the Suite interface, select **Administration**.
3. On the **Administration** page, click the **Synchronization** tab.

Figure 3.5: Set URL message



No Secondary Server Available

Must set current server URL before adding a secondary server

4. If you see the message *Must set current server URL before adding a secondary server*, you must configure the URL for the server. Click the message text to open the **Update Current Server** dialog.
5. In the **Update Current Server** dialog, set the value for the **Server URL**.
6. Click **Update**.

To modify the URL for the primary server:

1. Log in to the primary Protex server as a user with the administrator role.
2. In the Suite interface, select **Administration** in the user name menu.
3. On the **Administration** page, click the **Synchronization** tab.
4. From the server menu (next to the server name), select **Update Server URL**.

5. In the dialog, modify the **Server URL**.
6. Click **Update**.

✱ **To modify the URL for a secondary server:**

1. Log in to the primary Protex server as a user with the administrator role.
2. In the Suite interface, select **Administration** in the user name menu.
3. On the **Administration** page, click the **Synchronization** tab.
4. Click the expand icon (▶) next to the server name.
5. In the server menu, click **Modify Current Server**.
6. In the **Modify Current Server** dialog, modify the **Server URL**.
7. Optional: modify the **Server Name**.
8. Click **Update**.

3.6.3 Adding a Secondary Server for Synchronization

Use the following procedure to set up your Protex multi-server synchronization environment. There is no practical limit on the number of secondary servers you can add. All secondary servers must be running Protex 7.1 or higher.

To configure a secondary server, the following user roles are required:

- A user account with the administrator role and the server synchronization role on the primary server.
- A user account with the administrator role on the secondary server.

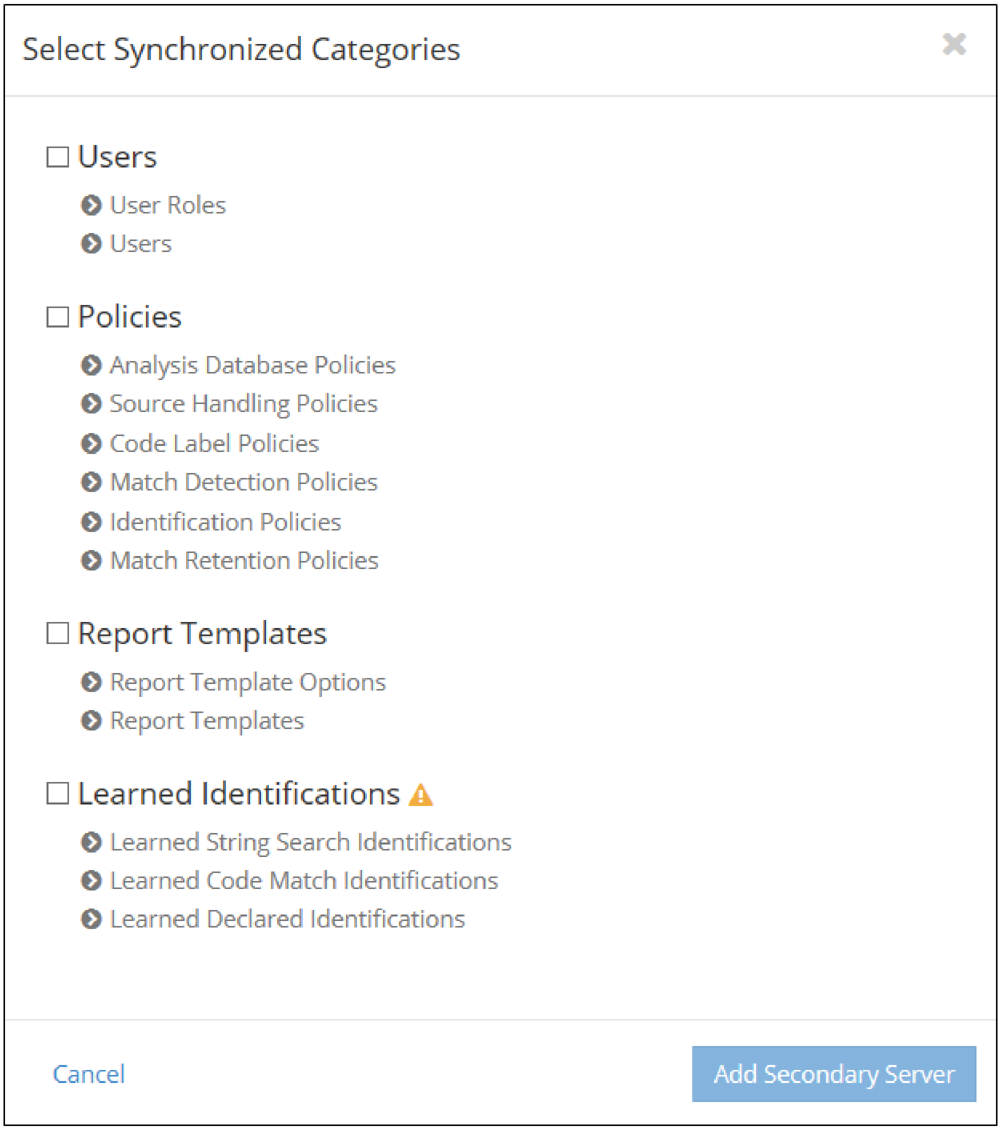
✱ **To add a secondary server to the synchronization environment:**

1. From the username menu in the Suite interface, select **Administration**.
2. On the **Administration** page, select the **Synchronization** tab.
3. On the **Synchronization** page, click the **Must set current server URL before adding a secondary server** link to open the **Modify Current Server** dialog.
4. In the **Modify Current Server** dialog, enter the:
   a. **Server URL**: This is the URL for your primary server.
   b. **Server Name**: *Optional:* The server URL is automatically entered as the server name. You can leave the server URL as the server name, or change the server name.
5. Click **Update**.
6. Click **Add Secondary Server**.
7. In the **Add Secondary Server** dialog, enter the:
   a. **Server URL**: This is the URL for your secondary server.

   b. **Server Name**: *Optional:* The server URL is automatically entered as the server name. You can leave the server URL as the server name, or change the server name.

8. Click **Next**.
9. In the **Connecting to Secondary Server** dialog, click **Login to Secondary Server**.
10. Enter the login credentials for the secondary server. In the **Do you want to grant access to your protected resources?** dialog, click **Authorize**.
11. In the **Select Synchronization Categories** dialog, select the categories to synchronize. Note that only the options supported by your versions of Protex are available. For more information, refer to Multi-Server Synchronization Data Options. Then click **Add Secondary Server**.

Figure 3.6: Select Synchronized Categories screen



Select Synchronized Categories ✕

□ Users

- User Roles
- Users

□ Policies

- Analysis Database Policies
- Source Handling Policies
- Code Label Policies
- Match Detection Policies
- Identification Policies
- Match Retention Policies

□ Report Templates

- Report Template Options
- Report Templates

□ Learned Identifications ⚠

- Learned String Search Identifications
- Learned Code Match Identifications
- Learned Declared Identifications

Cancel | Add Secondary Server

12. You are returned to the **Synchronization** tab. The name of the secondary server displays with a

green check mark status icon.

After a secondary server is added, the base import process automatically sends data from the primary server to the new secondary server. If there is a conflict, the data on the primary sever supersedes, as data on the secondary server is overwritten with data from the primary server.

3.6.4 Viewing the Status of Secondary Sync Servers

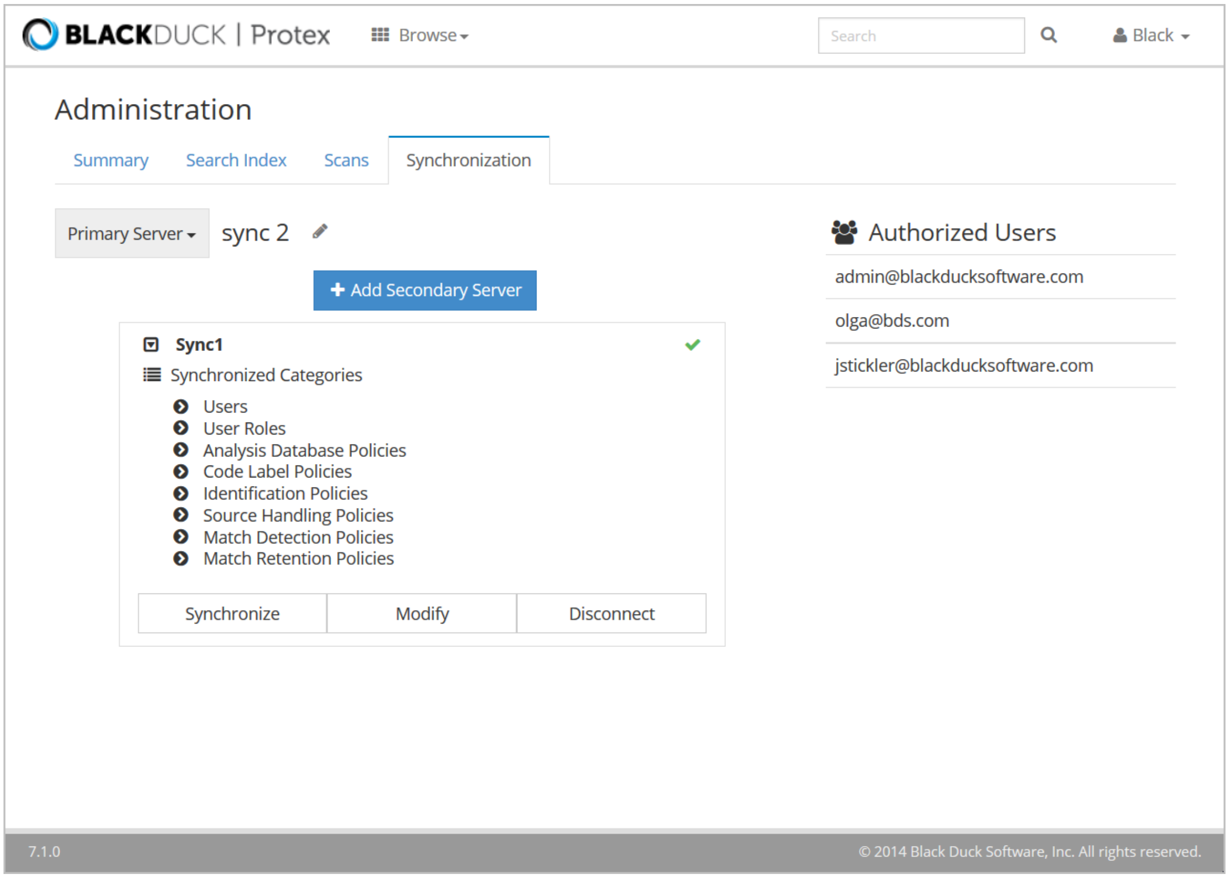
The **Administration** > **Synchronization** page in the Suite user interface displays information about your multi-server synchronization implementation. The data displayed differs based on viewing a primary server or a secondary server.

Primary Server	Secondary Server
Name or URL of the primary server. The server URL is a link to the login page for the secondary server.	Name or URL of the secondary server.
Names or URLs of the secondary servers that are synchronizing with this primary server.	Name or URL of the primary server with which this secondary server is synchronizing.
	Summary status of the secondary servers: • ✓: Online • ! or ⚠: Server issues • 🔁: Synchronizing • ✗: Offline
Synchronization Categories - Data configured to be synchronized on each of the primary servers.	Synchronization Categories - Data configured to be synchronized on the secondary server.
Users on the primary server who have the server synchronization role (that is, that can modify synchronized data on the primary server).	Users on the secondary server who have the server synchronization role (that is, that can modify synchronized data on this secondary server).

✱ To view the status of your secondary servers:

1. Log in to the Protex server as a user with the administrator and server synchronization roles.
2. From the user name menu, select **Administration**.
3. On the **Administration** page, click the **Synchronization** tab.

Figure 3.7: Administration > Synchronization screen



Administration

sync 2

Sync1 ✓

Synchronized Categories

- Users
- User Roles
- Analysis Database Policies
- Code Label Policies
- Identification Policies
- Source Handling Policies
- Match Detection Policies
- Match Retention Policies

Authorized Users

admin@blackducksoftware.com

olga@bds.com

jstickler@blackducksoftware.com

4. To view the synchronization categories for the secondary server, click the expand icon (▶) next to the server name.
5. To log in to the secondary server, click the server name.

3.6.5 Modifying the Configuration of a Secondary Server

You can modify the following properties for a secondary server:

- Server URL
- Server name

✱ To modify the configuration of a secondary server:

1. Log in to the primary Protex server as a user with the administrator role.
2. From the user name menu, select **Administration**.
3. On the **Administration** page, click the **Synchronization** tab.
4. Click the expand icon (▶) next to the server name.
5. Click **Modify Current Server**.

6. Modify the settings as needed.
7. Click **Update**.

3.6.6 Troubleshooting Multi-Server Synchronization

There are several troubleshooting and recovery options included in the multi-server synchronization feature.

Logging

There is a synchronization log (`synchronization_log`) on each server in a multi-server synchronization environment. These logs are visible on the **Tools** > **Admin Center** > **View Logs** page in the classic interface. To view full details for a logged event, click the event in the **View Logs** table. A new page displays, containing complete information for the logged event.

Protex logs before and after values for all synchronization updates. These values are logged at the default logging level (INFO).

Failure to update data on a secondary server is logged as an error in the logs on the primary server.

Failure to apply data changes on a secondary server are logged as an error in the logs on the secondary server.

Error messages

The following error/warning messages may appear on the **Synchronization** page. Each message has an associated action that you can take to attempt to correct problems.

Table 3.1: Error Messages

Message	Type	Description	Solution
Data Inconsistent	Error	A change was applied to the server, but the original data was in an unexpected and conflicting state. The server will attempt to auto-correct this issue, or the user may manually trigger a full synchronization.	For more information, refer to Manually Synchronizing Servers.
JMS Failure	Error	There has been a JMS issue communicating the with synchronized network. This is similar to a lost connection issue, but specifically within the JMS system.	1. Match the LDAP configuration with the other server. 2. Check the network connection with the other server. 3. Perform a full synchronization.
Lost Connection	Error	Communication has been lost with a synchronized server.	For more information, refer to Troubleshooting a Disconnected Server on

Message	Type	Description	Solution
			page 70.
Mismatched LDAP Configurations	Warning	Two synchronized servers do not have the same LDAP configuration. If users are synchronized, this may cause unexpected login behavior, such as the inability to log in through LDAP on one of the servers.	Match the LDAP configuration with the other server.

Manual Synchronization

If a secondary server gets into a state where there are data conflicts, you may receive the *Data Inconsistent* error message listed in the preceding table. In this case, you may want to manually trigger a full synchronization. The manual synchronization option forces a full synchronization, meaning that if there are data conflicts between the two servers, the data on the primary server overwrites the data on the secondary server. For more information, refer to Manually Synchronizing Servers.

Resetting a Server to Standalone Mode

If you have trouble removing a sever from a multi-server synchronization environment, Protex can force a hard reset of the server configuration back to that of a standalone Protex server. For more information, refer to Troubleshooting a Disconnected Server.

Clearing the JMS Message Persistent Store

This option should only be used if your system is down and you must recover from a completely corrupt message persistence store. If your message store is corrupted and unrecoverable, you can set this option to `True` for the system to automatically delete the existing persistence records before attempting to start, allowing a clean re-initialization.

Caution: All messages stored in the existing message persistence store are deleted when you perform this procedure.

✱ To clear the JMS message persistent data store:

1. On your server, navigate to the Tomcat startup file:

   ```
   /opt/blackduck/protexIP/config/bds-protexIP-tomcat.start
   ```

2. Open the file with a text editor.
3. Add the following text to the end of the file:

   ```
   export JAVA_OPTS=" -Dblackduck.messaging.clearPersistenceRecords=true
   ${JAVA_OPTS}"
   ```

Setting this property to `True` resets the JMS message store.

Note: On Windows, the Tomcat startup settings are configured in the following Windows Registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\protextc\Parameters\Java\

4. Save the file.
5. Restart Tomcat on the server.

Note: Each time the system starts with this system property set to `True`, the contents of the message store are deleted. As a best practice, you should allow the system to complete startup, and then edit your startup files to set the property back to `False` and restart Tomcat.

Manually Synchronizing Servers

Protex provides the option to manually synchronize a secondary server. This option forces a full synchronization, meaning that if there are data conflicts between the two servers, the data on the primary server overwrites the data on the secondary server. This provides a recovery option, in case the data on the secondary server must be reset.

✱ **To manually synchronize a secondary server from the primary server:**

1. Log in to the primary Protex server as a user with the administrator and server synchronization roles.
2. From the **User Name** menu, select **Administration**.
3. On the **Administration** page, click the **Synchronization** tab.
4. Click the expand icon (▶) next to the secondary server name.
5. Click **Synchronize**.
6. In the **Synchronize Secondary Server** dialog box, click **Synchronize Now**.

✱ **To manually synchronize a secondary server from the secondary server:**

1. Log in to the secondary Protex server as a user with the administrator and server synchronization roles.
2. From the **User Name** menu, select **Administration**.
3. On the **Administration** page, click the **Synchronization** tab.
4. Click the **Synchronize with Primary** button.
5. In the **Synchronize Secondary Server** dialog box, click **Synchronize Now**.

Disconnecting a Server from Synchronization

If the secondary server cannot communicate with the primary server, the synchronized data on the secondary server becomes locked for editing. Removing and re-adding the secondary server initiates a fresh data synchronization.

To disconnect a server from the primary server:

1. Log in to the primary Protex server as a user with the administrator role.
2. From the user name menu in the Suite interface, select **Administration**.
3. On the **Administration** page, click the **Synchronization** tab.
4. Click the expand icon (▶) next to the server name.
5. Click **Disconnect**.
6. In the **Confirm Disconnecting Secondary Server** dialog, click **Disconnect**.

To disconnect a server from the secondary server:

1. Log in to the secondary server as a user with the administrator role.
2. From the user name menu in the Suite interface, select **Administration**.
3. On the **Administration** page, click the **Synchronization** tab.
4. Click **Disconnect From Primary**.
5. In the **Confirm Disconnect From Primary** dialog, click **Disconnect**.

For more information regarding adding (re-connecting) the server after disconnecting , refer to Adding a Secondary Server for Synchronization on page 63.

Troubleshooting a Disconnected Server

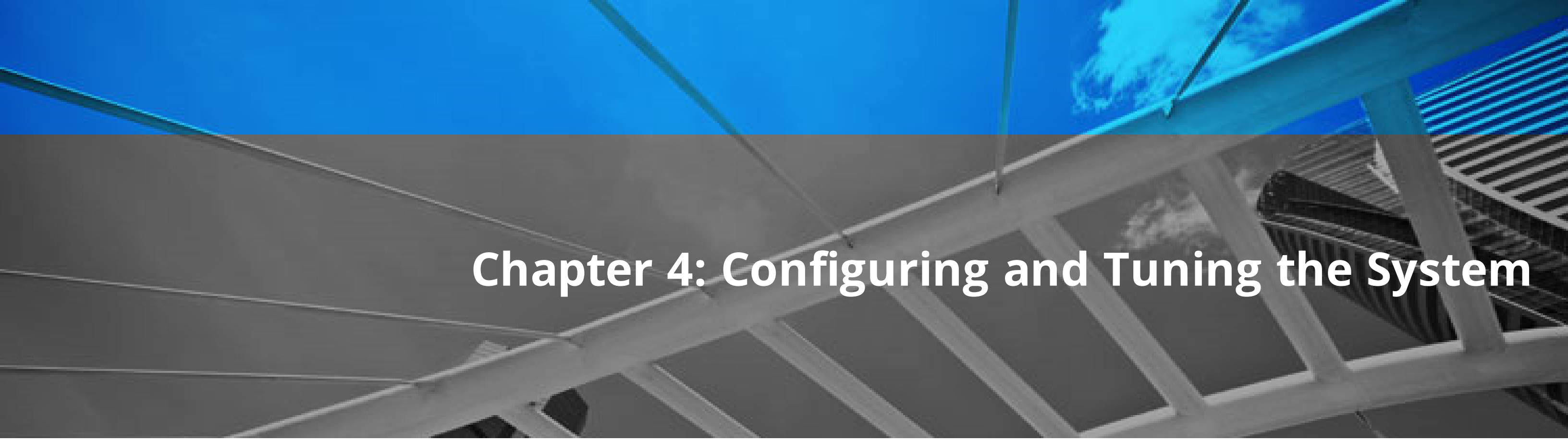
Under normal circumstances, disconnecting a server should be enough to remove it from a multi-server synchronization environment. However, if you have trouble removing a sever from a multi-server synchronization environment, Protex has an option to force a hard reset of the server configuration back to that of a standalone Protex server. This action stops subscriptions to the synchronization messaging queue, removes synchronization categories, and removes other synchronization-specific configurations from the server.

> **Note:** If the server is already a standalone server, the **Change to Standalone** option is not available.

To force a hard reset of a synchronized server back to a standalone Protex server:

1. Log in to the Protex server as a user with the administrator and server synchronization roles.
2. From the user name menu in the Suite interface, select **Administration**.
3. On the **Administration** page, click the **Synchronization** tab.
4. From the drop-down menu at the left of the server name, select **Change to Standalone**. Protex displays a message asking you to confirm that you want to convert the server.
5. In the **Change to Standalone** dialog box, click **To Standalone**. Protex converts the server to a standalone Protex server.

> **Note:** Converting a primary server back to a standalone server disconnects all secondary servers synchronized with this primary server.



Chapter 4: Configuring and Tuning the System

This chapter contains information about configuring and tuning Protex after completing the initial configuration of your Protex environment.

Unlike the initial configuration topics, you may need to repeat some of the procedures in this chapter as you fine-tune your Protex environment.

4.1 Stopping and Starting the Tomcat Server

There are instances where you need to stop and restart the Tomcat server. The following example outlines this process. It is divided into two phases, as follows:

- Stopping the Tomcat server
- Starting the Tomcat server

Note: Both of these phases require that you log in as root.

✱ To stop Tomcat:

1. Log in as root.
2. Enter the following command:

```
root@linux:~> /etc/init.d/bds-protexIP-tomcat stop
```

3. Ensure that all Tomcat processes have stopped by using the following command to check the process status:

```
root@linux:~> ps aux | grep tomcat
```

4. If the shell indicates that Tomcat is still running, enter the following command to delete the Tomcat lock:

```
root@linux:~> rm -f /var/lock/subsys/bds-protexIP-tomcat
```

✱ To start Tomcat:

1. Log in as root.
2. Enter the following start command:

```
root@linux:~> /etc/init.d/bds-protexIP-tomcat start
```

4.2 Setting Session Timeout Values

A property named `blackduck.ui.sessionTimeout` can be added to the `tomcat.start` file. This property provides system administrators with the ability to control user session timeouts when using Protex. System administrators can set the session timeout up to 1440 minutes (24 hours). We recommend that you do not set the value below 30 minutes due to possible performance issues.

> **Note:** If a page contains polling, the page does not timeout, as the inactive period is reset when the server responds to poll requests. This will be addressed in a future release.

✱ To set a UI session timeout value:

1. On the Apache Tomcat web server where the Black Duck application is running, open the `tomcat.start` file for editing.

   Linux:

   ```
   opt/blackduck/protexIP/config/bds-protexIP-tomcat.start
   ```

   On Windows, the Tomcat startup settings are configured in the following Windows registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache SoftwareFoundation\Procrun
   2.0\protextc\Parameters\Java\
   ```

2. To manage users session timeout in the Black Duck application, in the `tomcat.start` file, set the system property.

   Linux:

   ```
   export JAVA_OPTS="-Dblackduck.ui.sessionTimeout=(number of minutes)
   ${JAVA_OPTS}”
   ```

   Windows:

   ```
   -Dblackduck.ui.sessionTimeout=(number of minutes)
   ```

3. In Linux, save your changes to the `tomcat.start` file. In Windows, save and close the Registry Editor.

✱ To set a browser timeout value:

You can also set the timeout value for your browser. In the `tomcat` folder, modify the `web.xml` file according to the following examples. The default browser timeout value is 30 minutes, as shown in the following example.

```
<session-config>

     <session-timeout>30</session-timeout>

</session-config>
```

1. To set the browser timeout value to 60 minutes, edit the value as shown:

```
<session-config>

     <session-timeout>60</session-timeout>

</session-config>
```

2. To set the browser timeout value to never expire, edit the value as shown:

```
<session-config>

     <session-timeout>-1</session-timeout>

</session-config>
```

3. Then restart Tomcat as follows:

   - Windows: in Windows Services, find *Black Duck Protex Tomcat*; then stop and restart the service.
   - Linux: `/etc/init.d/bds-protexIP-tomcat restart`

4.3 PostgreSQL Tuning

This topic explains the PostgreSQL parameters and provides suggested values so you can tune your system accordingly.

Make copies of all configuration files prior to editing them. This ensures a base level to which you can fall back in case of serious issues.

Backup these configuration files:

- `postgresql.conf` — Located in the `/var/lib/bds-protexip/data` directory. To implement edits, you must stop and restart PostgreSQL for your changes to take effect. Note that `protexip` is all lowercase in this directory name.
- `/etc/init.d/bds-protexIP-postgresql` — Checks the configured `shmmax` value and corrects it if required, based on the amount of physical memory of the server at installation time.

The following table provides details for each PostgreSQL parameter. It includes a brief description about the parameter, and states suggested values for the tuning process.

> **Note:** The dynamic values are automatically configured during installation, based on the physical memory in the system. The dynamic installation parameters are defined in the following table.

Table 4.1: PostgreSQL Parameters

Parameter	Description

`checkpoint_ segments`
`(static)`
	This parameter specifies the WAL files available for use with checkpoints. The WAL files are stored in `/var/lib/bds-protexip/data/pg_xlog`. Larger values help performance when database activity is busy. Larger values also increase startup time when recovering from abnormal termination.
	Note: PostgreSQL log files contain a message if the checkpoint segments are too close or too frequent.

`effective_ cache_size`
`N KB (set by installer)`
	This parameter informs the query optimizer of the amount of operating system file system cache you expect to have available. The default is to use 50% of free memory.

`maintenance_ work_mem`
`N KB (set by installer)`
	This parameter specifies the maximum amount of memory to be used in maintenance operations (such as VACUUM). The default is 256 MB per 4GB of system memory.
	Note: Similar to `work_mem`, this incorporates other tasks into its usage beyond the parameter it replaces.

`max_ connections`
`200`
	This parameter specifies the number of concurrent connections possible to this database. Typically, you should stay with the default unless you get a fatal error stating that the connection limit has been exceeded for non-superusers.

`Random_page_ cost`
`(static)`
	If you have particularly fast disks, as commonly found with RAID arrays of SSD disks, it may be appropriate to lower this figure, which encourages the query optimizer to use random access index scans. The default is 4.0.

`Shared_ buffers`
`200000 KB per 4GB of memory (set by installer)`
	Shared buffers contain query results that are in progress. A good estimate is between 5% and 15% of total system memory, but no more than 8GB.
	Note: This value does not include operating system file caching. Refer to `effective_ cache_size`.

`work_mem`
`131077 KB per 4GB of memory (set by installer)`
	Increasing this parameter allows PostgreSQL to do larger in-memory sorts which are faster than disk-based equivalents.
	Keep in mind that this size is applied to all sorts done by each user. Set it to 50MB, and have 30 users submitting queries, and you are soon using 1.5GB of real memory.

4.3.1 Move the Write Ahead Log (WAL) Files

Caution: If you decide to move the WAL files, turn off PostgreSQL before starting the move. Otherwise, a total loss of the entire database can occur. Contact Black Duck Services to have them perform this operation.

Moving WAL files to a separate, dedicated drive can increase the performance by reducing the seek times on the main database drives.

Note: The following example assumes that the WAL drive is mounted on `/u1`.

✱ To move the WAL files:

1. Set up a directory for the new WAL location:

```
mkdir -p /u1/pgsql
```

2. Change owner of the directory by issuing the following command:

```
chown bds-protexIP /u1/pgsql
```

3. Change permissions of the directory by issuing the following command:

```
chmod 700 /u1/pgsql
```

4. Make backup copies of `bds_customer` and `fp_customer` databases.
5. Verify that PostgreSQL is stopped.

Caution: Failure to stop PostgreSQL can result in a total loss of the entire database.

6. Change to the PostgreSQL data directory:

```
cd /var/lib/bds-protexip/data
```

7. Copy the WAL directory to the new location:

```
cp -a pg_xlog /u1/pgsql
```

8. Rename the current WAL directory to:

```
mv pg_xlog pg_xlog.old
```

9. Create a symbolic link to the new location, using the command:

```
ln -s /u1/pgsql/pg_xlog .
```

10. Restart PostgreSQL. After PostgreSQL restarts, the contents of the old WAL directory can no longer be used. Verify that PostgreSQL is running.
11. After restarting PostgreSQL, delete the file:

```
rm -rf pg_xlog.old
```

4.4 Managing Disk Space

As described in the *Protex Installation Guide*, Black Duck recommends a server system with two storage arrays, and a separate partition for the `/opt` directory. This directory can grow quite large with usage, as shown in the following table.

Table 4.2: Directory Usage

Directory	Usage
`/opt/blackduck/protexIP/source`	Code printing stores reference source files here.
`/opt/blackduck/protexIP/searchreport`	Used for the string search index. The size increases for larger code bases.
`/opt/blackduck/protexIP/downloads`	Contains files used for Black Duck updates. By default, these are automatically deleted. If you change the default and keep the old updates, periodically monitor

Directory	Usage
	the storage capacity of this directory.
/opt/blackduck/tomcat/logs/Catalina.out /opt/blackduck/tomcat/logs/blackduck_log.txt.<date> /opt/blackduck/tomcat/logs/blackduck_access_log.<date>.txt	Tomcat log files grow continuously, and are not managed from within Protex. You should periodically purge these files.

If you run out of disk space, one option is to create a symbolic link from the /opt/blackduck/protexIP directory to another location with more free space. For example, if your users are going to be doing extensive code printing, then you may want to create a symbolic link in the /opt/blackduck/protexIP directory to a disk with more free space.

Command syntax is:

```
ln -s target directory
```

To create symbolic link in this example, issue the following command:

```
ln -s /home/user/sourceLn /opt/blackduck/protexIP
```

This example creates a link in /opt/blackduck/protexIP to sourceLn in your home directory.

When adding space in this way, the minimum extra space that to allocate is 2 GB.

Another option for additional disk space is mounting an additional drive to the /var/lib/bds-protexip directory.

4.4.1 Configuring Memory Options

On occasion when analyzing extremely large code bases, you can exceed the default memory configured for Protex. The Protex client software tools (**bdstool**, **bdsscan**, and **bdscompare**) are Java clients using the default heap size of the Java Virtual Machine.

Under these circumstances, you may want to allocate more memory to Protex and change the heap size to a larger value.

Each of the Protex client tools utilizes environment variables that can be used to override the default Java settings. The following table lists the relevant environment variables.

Table 4.3: Environment Variables

Variables and Arguments	Description
bdsjavaoptions	Used to override Java options in all Protex tools.
bdscomparejavaoptions	File comparison tool only.
bdstooljavaoptions	Command line interface only.
bdsscanjavaoptions	Web application scanning only.

Variables and Arguments	Description
-Xms (size in bytes)	Sets the initial size of the Java heap. The default size is 2097152 (2MB). The values must be a multiple of, and greater than, 1024 bytes (1KB).
-Xmx (Size in bytes)	Sets the maximum size to which the Java heap can grow. The default size is 64MB.

Examples

To increase the client process memory range from 5MB to 128MB, set the following environment variable in your users .bashrc file, located in your home directory:

```
export bdsjavaoptions='-Xms5m -Xmx128m'
```

If you only want to change the memory for the file comparison tool, set the following environment variable:

```
export bdscomparejavaoptions='-Xms5m -Xmx128m'
```

✱ To set an environment variable under Linux:

1. In bash, update /etc/profile file by inserting the following lines:

   ```
   export <variable name>='<value>'
   (example: export BDSJAVAOPTIONS=' -Xmx512m')
   ```

2. In tcsh, update the /etc/csh.login file by inserting the following line:

   ```
   setenv <variable name> <value>
   ```

   For example:

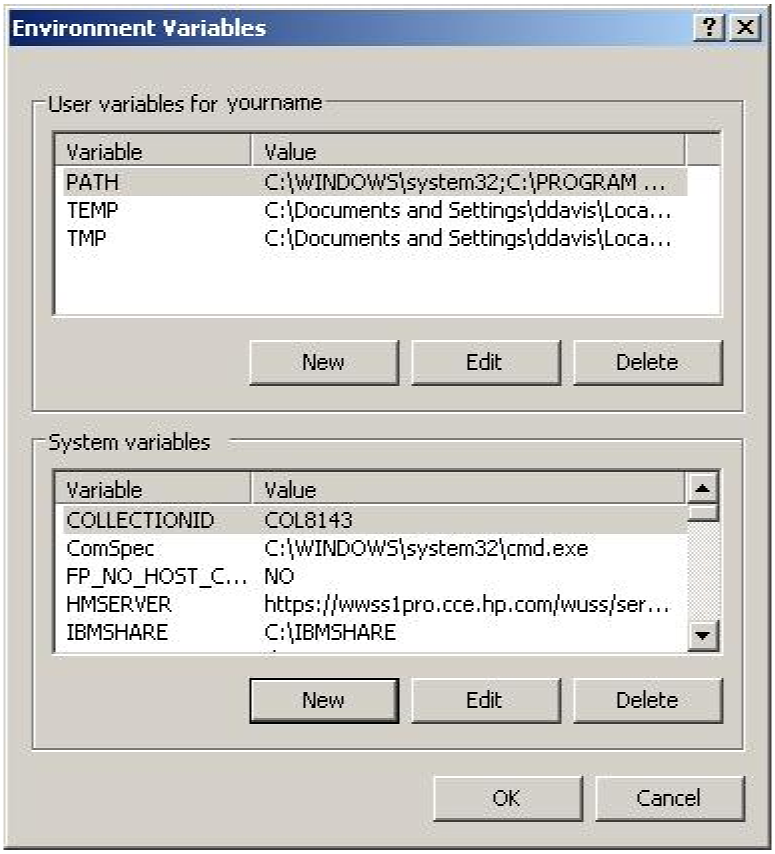
   ```
   setenv BDSJAVAOPTIONS '-Xmx512m'
   ```

3. Log out and back in to initiate the change.

✱ To set an environment variable under Windows:

1. Select **Start** > **Control Panel**. The **Control Panel** opens.
2. Select **System**. The **System Properties** dialog opens.
3. Select the **Advanced** tab.
4. Click **Environment Variables**. The **Environment Variables** dialog opens.

Figure 4.1: Environmental Variables dialog



Environment Variables

User variables for yourname

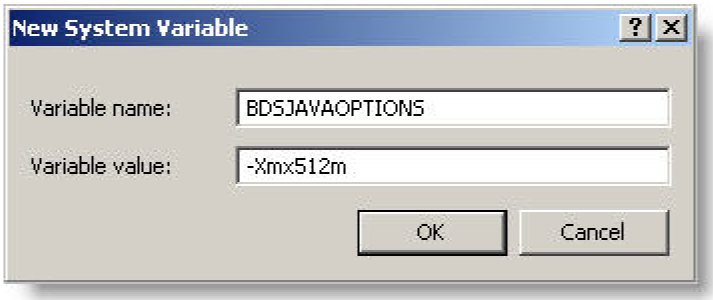
Variable	Value
PATH	C:\WINDOWS\system32;C:\PROGRAM ...
TEMP	C:\Documents and Settings\ddavis\Loca...
TMP	C:\Documents and Settings\ddavis\Loca...

System variables

Variable	Value
COLLECTIONID	COL8143
ComSpec	C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_C...	NO
HMSERVER	https://wwss1pro.cce.hp.com/wuss/ser...
IBMSHARE	C:\IBMSHARE

5. In the System Variables section, click **New**. The **New System Variable** dialog opens.

Figure 4.2: New System Variable dialog



New System Variable

Variable name: BDSJAVAOPTIONS

Variable value: -Xmx512m

6. Enter the variable name and value and click **OK**. The **New System Variable** dialog closes.
7. Click **OK**. The Environmental Variables dialog displays, and the new variable appears in the list.
8. Click **OK** to return to the **Control Panel**.

4.5 Configuring Server File Access

File server access is a configurable option in Protex. By default this feature is enabled, granting users the full functionality of Protex. Server file access lets you browse the Black Duck home directory on the

Protex server for any code placed there for analysis. Typical usage leaves this option enabled.

Disabling server file access restricts you to analyzing projects locally and also limits you to just browsing the server if restricted.

You must have the administrator or manager role to perform this action.

✱ **To set server file access:**

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Policy Manager**. Protex displays the **General** tab of the **Policy Manager**.
4. In the **Server File Access** section, select or clear the **Allow Server File Access** check box.

   Note: Deselecting server file access restricts users to analyzing projects locally.

5. Click **Save**.

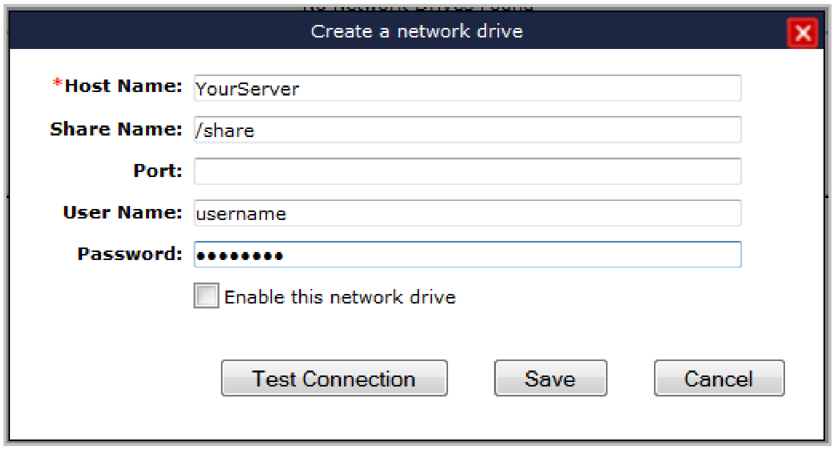
4.6 Analyzing Code on Network Drives

For analysis, Protex stores your code in one of two locations: directly on the Protex server machine, or on a local disk accessible by a Protex client. A third option is to use a network drive accessible from the Protex server.

✱ **To configure Protex to analyze code on a network drive:**

1. From a system directly connected to the drive, share the resource as appropriate for your operating system.
2. Log in to your Protex server.
3. From the user name menu in the **Suite** interface, select **Administration**.
4. On the **Administration** > **Summary** page, click **Network Drive Configuration**.
5. In the Classic interface, on the **Tools** > **Admin Center** > **Configuration** page, click **Add a network drive**. The **Create a network drive** dialog opens.

Figure 4.3: Create Network Drive



*Host Name: YourServer

Share Name: /share

Port:

User Name: username

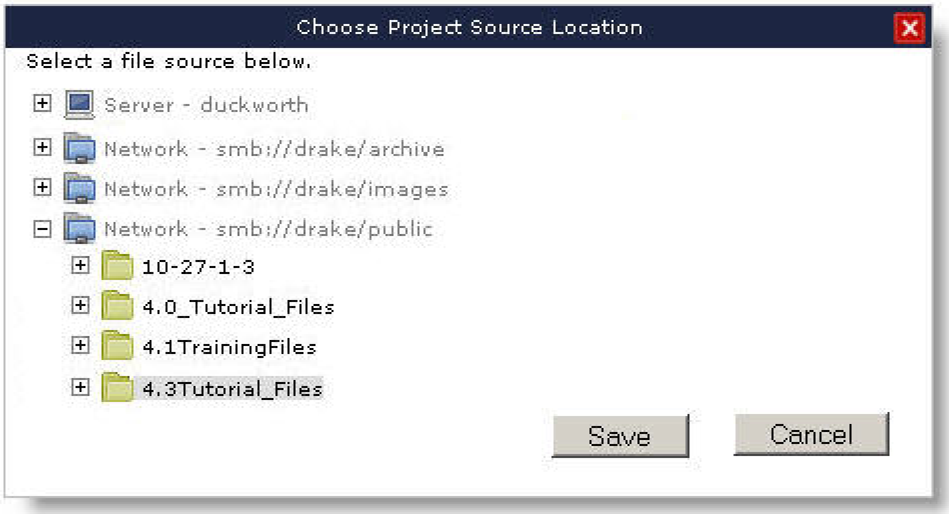
Password: ••••••••

□ Enable this network drive

6. Enter the information for your drive:
7. Click the **Enable this network drive** check box.
8. Click **Test Connection**. Protex attempts to connect to the network drive and displays a success or failure message.
9. Click **Save**. The network drive is immediately visible in the **Network Drive** table on the **Tools** > **Admin Center** > **Configuration** page.

Tip: When using a samba server, you must create a GUEST account on that server with no password to use anonymous access.

Figure 4.4: Server and Network Drives



Select a file source below.

- Server - duckworth
- Network - smb://drake/archive
- Network - smb://drake/images
- Network - smb://drake/public
  - 10-27-1-3
  - 4.0_Tutorial_Files
  - 4.1TrainingFiles
  - 4.3Tutorial_Files

Note: Previously, the configuration of network drives required a `root.properties` file. As of Protex 6.0, this is no longer required. When you first start Protex, it reads the old configuration file and loads the drive information into the new area. After confirming that the drive details are entered, delete the `/opt/blackduck/protexIP/config/root.properties` file.

4.7 Customizing the User Interface

The following sections show how to customize your Protex user interface. These changes are made on a server basis and a restart of Tomcat is required.

4.7.1 Customizing Tab and Label Text

It is possible to change many of the text strings appearing in the user interface, including tab names. You can do this by creating a new `message.properties` file that supersedes the default file.

Tip: A common change might be to add a message to the Protex login screen telling users how to request an account. For example: `ProtexLoginPageGreetingMessage`=For access please contact the Compliance Team at x1234

The standard text strings are stored in: `/opt/blackduck/protexIP/config/default.messages.properties`. Open this file to find the name of the text field you want to change, but do not edit this file. Instead, create a new `messages.properties` file in that same directory and make your changes there.

Example

✱ **To change the text on the dashboard from *Select a Project* to *Hello World*:**

1. In the `/opt/blackduck/protexIP/config/` directory, create a text file named `messages.properties`.
2. Add the following line to your new file:

```
ProtexIPStartPageHeaderText=Hello World
```

3. Restart Tomcat.

If necessary, you can put the new `messages.properties` file in a different location. In this case, you must tell Protex where to find the new (override) file. Add the following line to your `/opt/blackduck/protexIP/config/bds-protexIP-tomcat.start` file:

```
-Dblackduck.ui.messagesFileLocation=/<mypath>/messages.properties
```

Note: On Windows, the Tomcat startup settings are configured in the following Windows Registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\protextc\Parameters\Java\

You must restart Tomcat when making these types of changes to your Protex server.

> **Note:** Do not copy the entire `default.messages.properties` file into the override file. This causes future label changes in the product to be overridden by the previous version's default values. Instead, create a new file and only include the individual lines for the label keys that you want to override.

4.7.2 Changing Date Formats

Protex displays dates in one of three formats:

- November 09, 1978
- November 09, 1978 02:47:12 PM
- 1978-11-09

These formats correspond to the following entries in the `default.messages.properties` file:

- GLOBALFormatDate=MMMM dd, yyyy
- GLOBALFormatDateTime=MMMM dd, yyyy hh:mm:ss a
- GLOBALFormatISODate=yyyy-MM-dd

You can override these formats using a custom `messages.properties` file. For example, depending on your local preference, you could change the date from yyyy-MM-dd to MM-dd-yyyy.

Refer to the Google Web Toolkit documentation at: http://google-web-toolkit.googlecode.com/svn/javadoc/1.6/com/google/gwt/i18n/client/DateTimeFormat.html for date format option information.

Chapter 5: Managing Protex

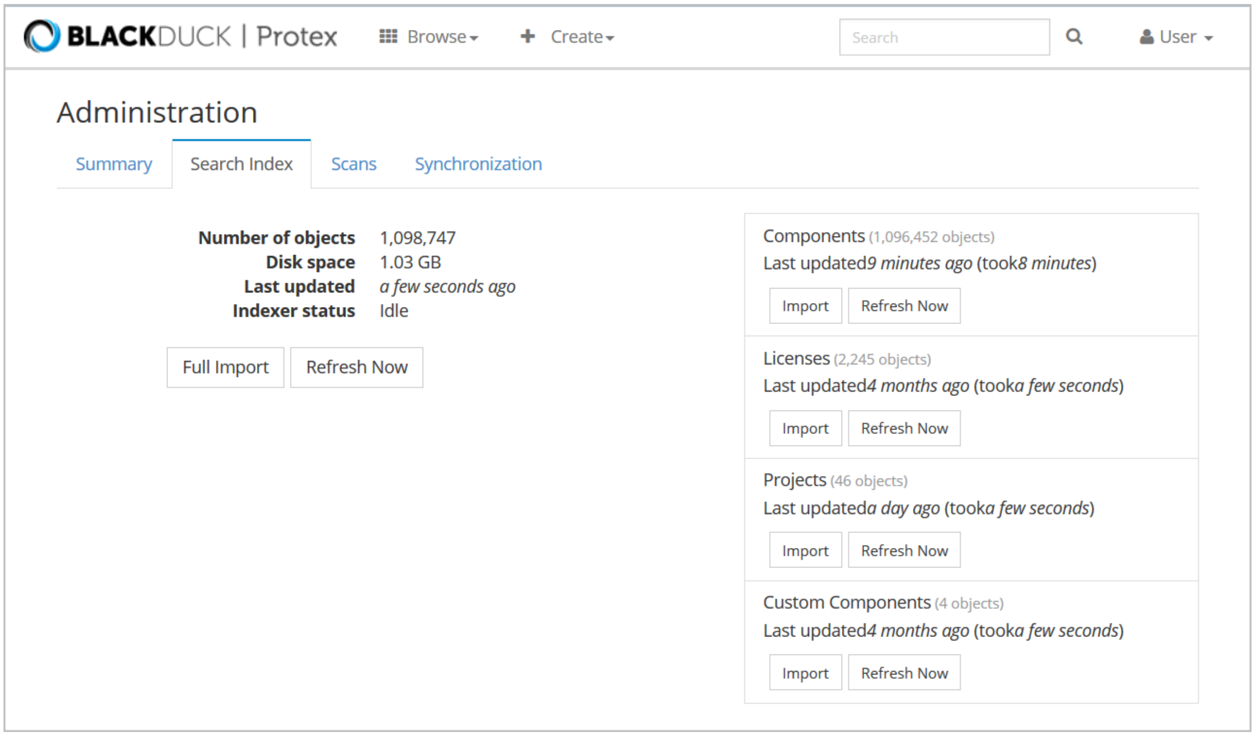
This chapter contains information about system administration for your Protex system.

5.1 Managing Solr Indexes

Protex uses Apache Solr to provide the ability to search across projects, components, custom components, and licenses, and filter by individual facets of your search.

Manage the Solr index from the **Administration** > **Search Index** page in the Suite interface.

Figure 5.1: Solr Search Index Administration Page



Administration

Number of objects 1,098,747
Disk space 1.03 GB
Last updated *a few seconds ago*
Indexer status Idle

Components (1,096,452 objects)
Last updated*9 minutes ago* (took*8 minutes*)

Licenses (2,245 objects)
Last updated*4 months ago* (tooka *few seconds*)

Projects (46 objects)
Last updated*a day ago* (tooka *few seconds*)

Custom Components (4 objects)
Last updated*4 months ago* (tooka *few seconds*)

5.1.1 Building a Solr Index

If you have an existing Protex installation and have upgraded to Protex 7, you will need to manually build the Solr indexes before users can use the faceted search in the Suite interface. Running a full import will query your Protex database and create a Solr index from scratch.

Note: You must have the Administrator role to perform this action.

✱ **To build a new Solr index, do the following:**

1. Log in to Protex.
2. From the user name menu in the **Suite** interface, select **Administration**..
3. Click the Search Index tab.
4. Click the **Full Import** button. Protex imports the data from your Protex database and builds the Solr index.

5.1.2 Refreshing a Solr Index

Once you have built your initial Solr index, as new data is added to your Protex server you can choose to recreate the entire index, or to refresh one or more facets of your index.

When you refresh the index, Protex queries the database for changes since the last time the index was build and then adds them to the existing index. Refreshing the index is therefore a much faster operation than a full import, as you're only indexing the changes since the last time the index was built or refreshed.

You have the option to refresh the entire Solr index, or you can refresh your index one facet at a time. When you choose to refresh a facet of the index, for example Components, the other facets of the index are not changed.

Note: You must have the Administrator role to perform this action.

✱ **To refresh one or more facets of your Solr index, do the following:**

1. Log in to Protex.
2. From the user name menu in the **Suite** interface, select **Administration**..
3. Click the Search Index tab.
4. Click the **Refresh Now** button for either the entire index, or the facet that you want to re-index.

5.2 Backing Up the Protex Databases

System backup is an important, yet sometimes overlooked, operation. Files are deleted, or a power failure interrupts your work in a project. Consequently, your data is only as good as your last backup. You must be diligent about preserving data on a regular basis.

A regular backup routine is an essential element of system administration. This chapter contains details to simplify the task - including restore procedures.

This chapter describes database backup procedures for your Protex server. Some databases should be backed up on a daily basis, and others can be backed up less frequently. Protex Database Names on page 85 provides a list of the databases and the recommended backup frequency. For exact instructions on how to perform these backups, refer to:

- Database Backup Procedure - Linux on page 86
- Database Backup Procedure - Windows on page 87

For information on the restore procedures, refer to:

- Restoring the Database - Linux on page 92
- Restoring the Database - Windows on page 93

Additionally, include the following files/directories in your normal system backups:

```
/opt/blackduck/protexIP
zip -r blackduck /opt/blackduck/protexIP
/var/lib/bds-protexip/data/p*
```

The Protex backup process is simple, but requires some manual steps on your part.

5.2.1 Protex Database Names

The following table lists the Protex databases and their recommended backup frequencies.

Table 5.1: Database Names and Backup Frequencies

Database Name	Description	Backup Frequency
bds_basic	(read-only) Contains product and standard KnowledgeBase information, including project and release information.	Back up after every KnowledgeBase update.
fp_basic	(read-only) Contains codeprint (fingerprint) information for the projects in the KnowledgeBase.	Back up after every KnowledgeBase update.
bds_customer	Contains customer configuration data, including users and projects.	Back up daily.
fp_customer	Contains customer codeprints; in other words, custom codeprints or fingerprints.	Back up after codeprinting. **Important:** The fp_customer database must always be synchronized with the bds_customer database. If you need to restore fp_customer, you must also restore the corresponding bds_customer (of the same date or newer) from the same system.

Note: Because the Solr index can be rebuilt from the bds_customer and bds_basic databases, there is no requirement to back up your Solr indexes in Protex.

✱ To see all the databases in the system:

1. Change to the bds-protexip user with this command:

   ```
   root@linux~> su - bds-protexip
   ```

   Your prompt changes to indicate the new user, and your current directory changes to /var/lib/bds-protexip.

2. Enter the following command to list the databases:

```
psql -l
```

A list of databases displays.

5.2.2 Database Backup Procedure - Linux

Back up the most important data first and label your backup media carefully. The standard process for backing up a PostgreSQL database is to dump it to a file. This serves as your backup. You may want to copy your backup files to removable media such as tape or DVD. Should you lose data, or if a database gets corrupted, you can restore the database using this file.

Note: Consider performing backup procedures during off hours when no one is using the system. Stop Tomcat before performing backups.

The process begins with the creation of the dump file, described as follows.

✱ To back up the PostgreSQL database on Linux:

1. Log in as root.
2. Stop Tomcat. This ensures a self-consistent backup.

```
root@linux~> /etc/init.d/bds-protexIP-tomcat stop
```

3. Change to the *bds-protexip* user.

```
root@linux~> su - bds-protexip
```

Your prompt changes to indicate the new user, and your current directory changes to `/var/lib/bds-protexip`.

4. Enter the following command to dump to a compressed file. Dump the database to a location with sufficient free space; this example uses `/tmp`. Also, this command ignores several scratch tables that do not require backing up:

```
pg_dump -Fc -T 'rpuid_*.custom_codetree_*_*'
-T 'rpuid_*.custom_file_*_*'
-T 'rpuid_*.custom_rawdiscoveryprofile_*_*'
-T 'rpuid_*.custom_compressedrawdiscoveryprofile_*_*'
-f /tmp/bds_customer.dump bds_customer
```

This puts the information from the `bds_customer` database into a file called `bds_customer.dump` in the `/tmp` directory.

5. Take the `bds_customer.dump` file and save it to another system or removable media.
6. Change back to the root user and restart Tomcat:

```
su
root@linux~> /etc/init.d/bds-protexIP-tomcat start
```

Repeat this process for each database, providing a unique name for each backup file.

Tip: If you find that dumping the database takes too long, you can greatly increase the backup speed by dumping to an uncompressed file. The trade-off is that while the dump process can be up to three times faster, the resulting file may be four times larger. To experiment with this on your system, add the `--compress=0` parameter to your `pg_dump` command.

5.2.3 Database Backup Procedure - Windows

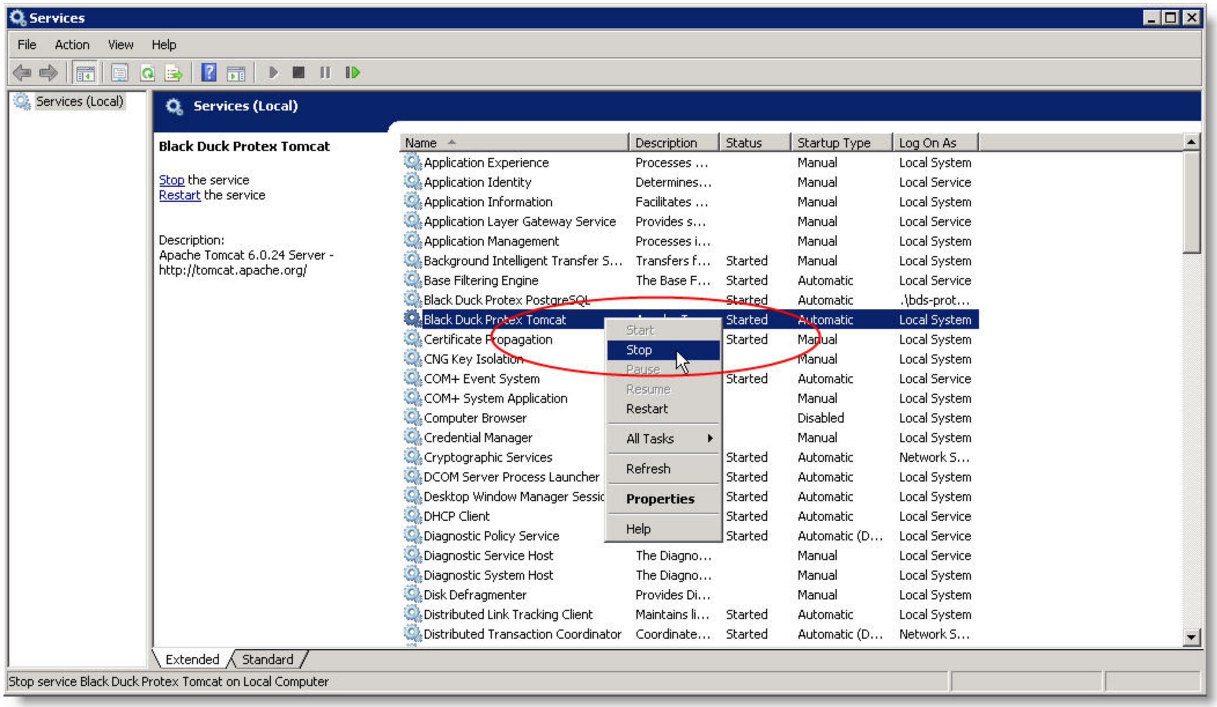
Note: This procedure requires a database password. Contact Black Duck Customer Support for the password for your database. Call +1 781.891.5100, extension 5.

On Windows systems, you can use the **pgAdmin III** tool to back up your databases. This tool is included with the Protex installation.

To back up the PostgreSQL database on Windows:

1. Login to the machine hosting the Protex server.
2. Stop the Black Duck Tomcat service.

Figure 5.2: Black Duck Tomcat Service



Black Duck Protex Tomcat

Stop the service
Restart the service

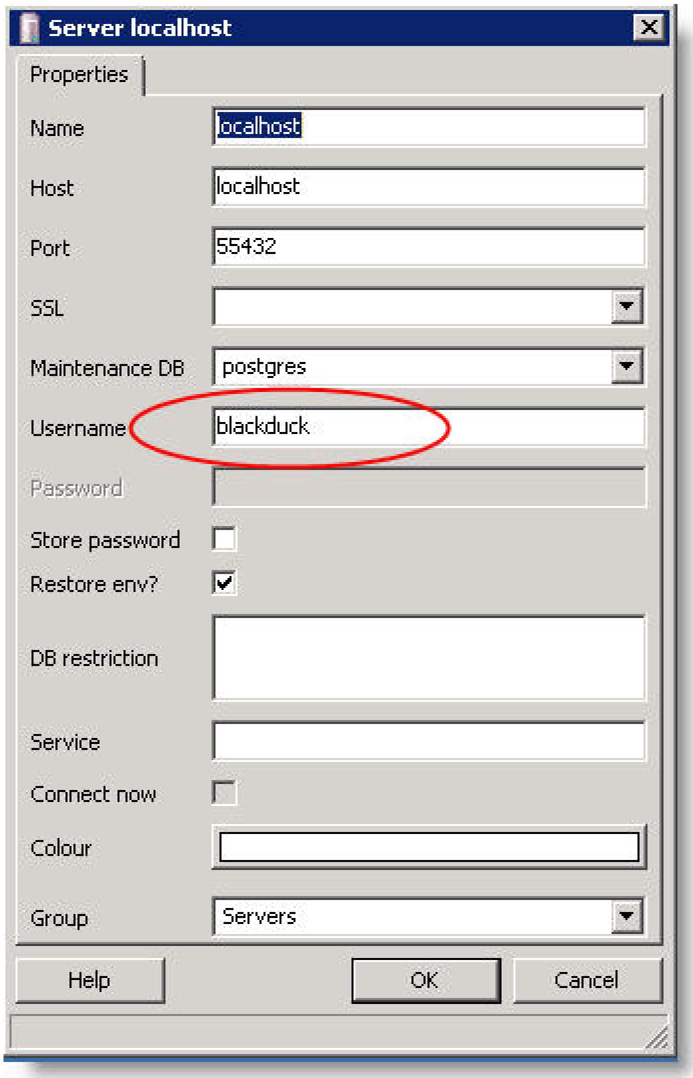
Description:
Apache Tomcat 6.0.24 Server - http://tomcat.apache.org/

Name	Description	Status	Startup Type	Log On As
Application Experience	Processes ...		Manual	Local System
Application Identity	Determines...		Manual	Local Service
Application Information	Facilitates ...		Manual	Local System
Application Layer Gateway Service	Provides s...		Manual	Local Service
Application Management	Processes i...		Manual	Local System
Background Intelligent Transfer S...	Transfers f...	Started	Manual	Local System
Base Filtering Engine	The Base F...	Started	Automatic	Local Service
Black Duck Protex PostgreSQL		Started	Automatic	.\bds-prot...
Black Duck Protex Tomcat		Started	Automatic	Local System
Certificate Propagation		Started	Manual	Local System
CNG Key Isolation			Manual	Local System
COM+ Event System		Started	Automatic	Local Service
COM+ System Application			Manual	Local System
Computer Browser			Disabled	Local System
Credential Manager			Manual	Local System
Cryptographic Services		Started	Automatic	Network S...
DCOM Server Process Launcher		Started	Automatic	Local System
Desktop Window Manager Sessic		Started	Automatic	Local System
DHCP Client		Started	Automatic	Local Service
Diagnostic Policy Service		Started	Automatic (D...	Local Service
Diagnostic Service Host	The Diagno...		Manual	Local Service
Diagnostic System Host	The Diagno...		Manual	Local System
Disk Defragmenter	Provides Di...		Manual	Local System
Distributed Link Tracking Client	Maintains li...	Started	Automatic	Local System
Distributed Transaction Coordinator	Coordinate...	Started	Automatic (D...	Network S...

Stop service Black Duck Protex Tomcat on Local Computer

3. Go to **Start** > **All Programs** > **PostgreSQL** > **pgAdmin III**, and start the **pgAdmin** tool.
4. Right-click the localhost database, and choose **Properties**.
5. If necessary, change the user name to *blackduck*, and click **OK**. This is a privileged user account for accessing the database.

Figure 5.3: blackduck username



Name: localhost

Host: localhost

Port: 55432

SSL:

Maintenance DB: postgres

Username: blackduck

Password:

Store password: □

Restore env?: ☑

DB restriction:

Service:

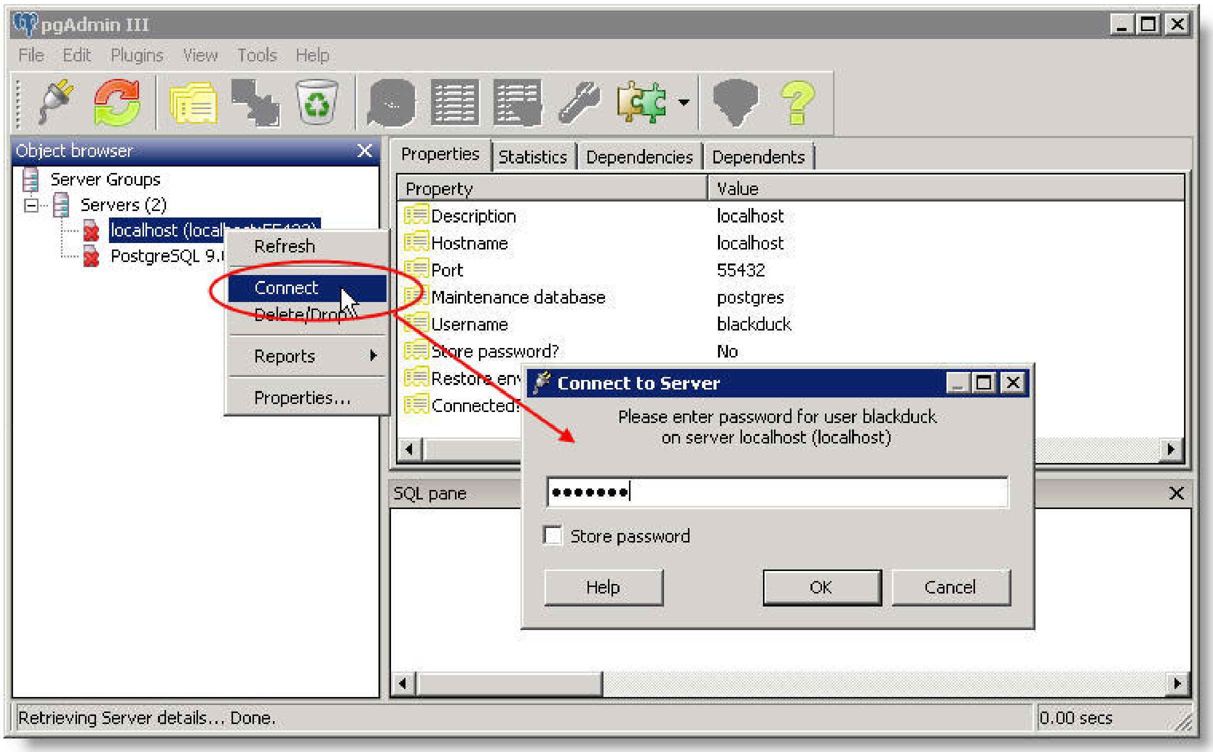
Connect now: □

Colour:

Group: Servers

6. Next, right-click the localhost database, and choose **Connect**. Enter the password you obtained from Black Duck Customer Support.

Figure 5.4: Connect to Server



Property	Value
Description	localhost
Hostname	localhost
Port	55432
Maintenance database	postgres
Username	blackduck
Store password?	No
Restore env	
Connected?	

Connect to Server

Please enter password for user blackduck
on server localhost (localhost)

•••••••

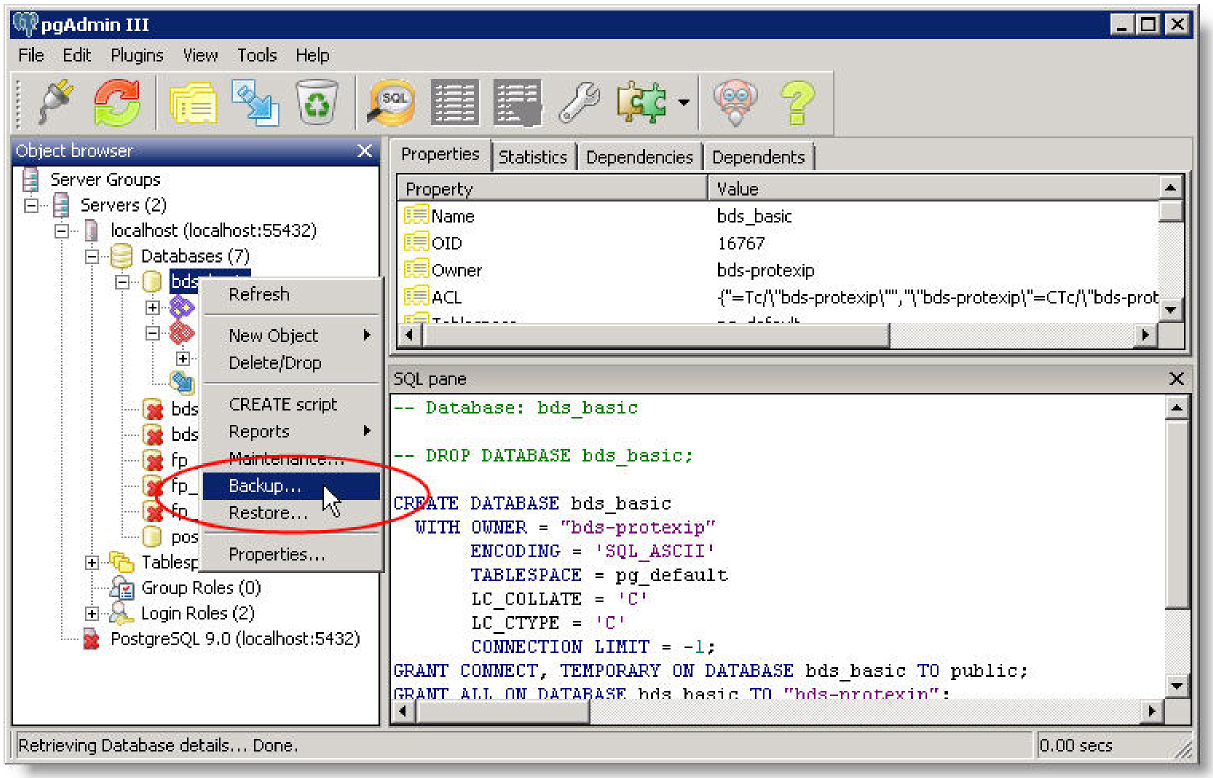
□ Store password

Retrieving Server details... Done.

0.00 secs

7. Right-click the **bds_basic database** and choose **Backup**.

Figure 5.5: Backup server



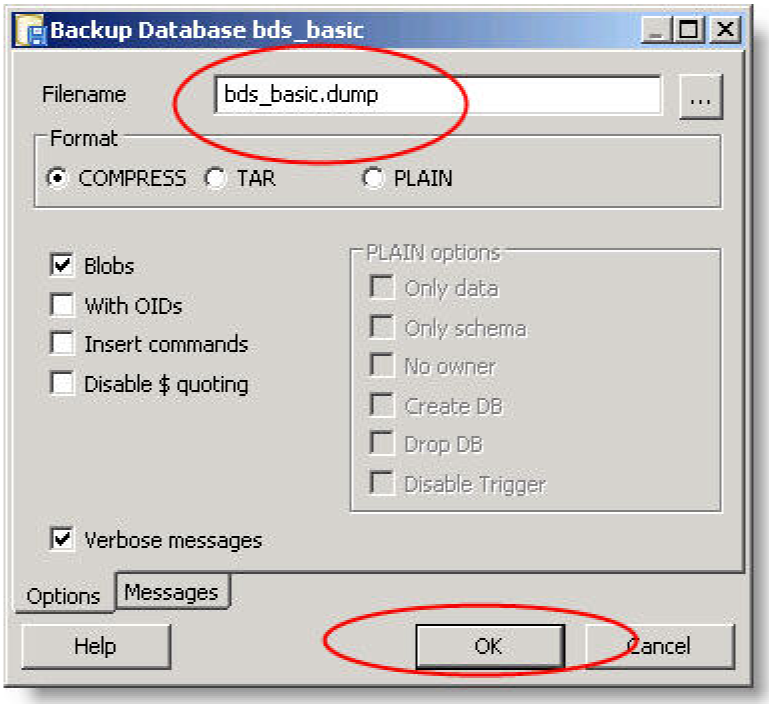
Property	Value
Name	bds_basic
OID	16767
Owner	bds-protexip
ACL	{"=Tc/\"bds-protexip\"","\"bds-protexip\"=CTc/\"bds-prot

```
-- Database: bds_basic

-- DROP DATABASE bds_basic;

CREATE DATABASE bds_basic
  WITH OWNER = "bds-protexip"
       ENCODING = 'SQL_ASCII'
       TABLESPACE = pg_default
       LC_COLLATE = 'C'
       LC_CTYPE = 'C'
       CONNECTION LIMIT = -1;
GRANT CONNECT, TEMPORARY ON DATABASE bds_basic TO public;
GRANT ALL ON DATABASE bds_basic TO "bds-protexip";
```

Retrieving Database details... Done. 0.00 secs

8. Enter a unique name for the backup file, such as *bds_basic.dump*, and click **OK**.

Figure 5.6: bds_Basic.dump



Backup Database bds_basic

Filename: bds_basic.dump

Format: ● COMPRESS ○ TAR ○ PLAIN

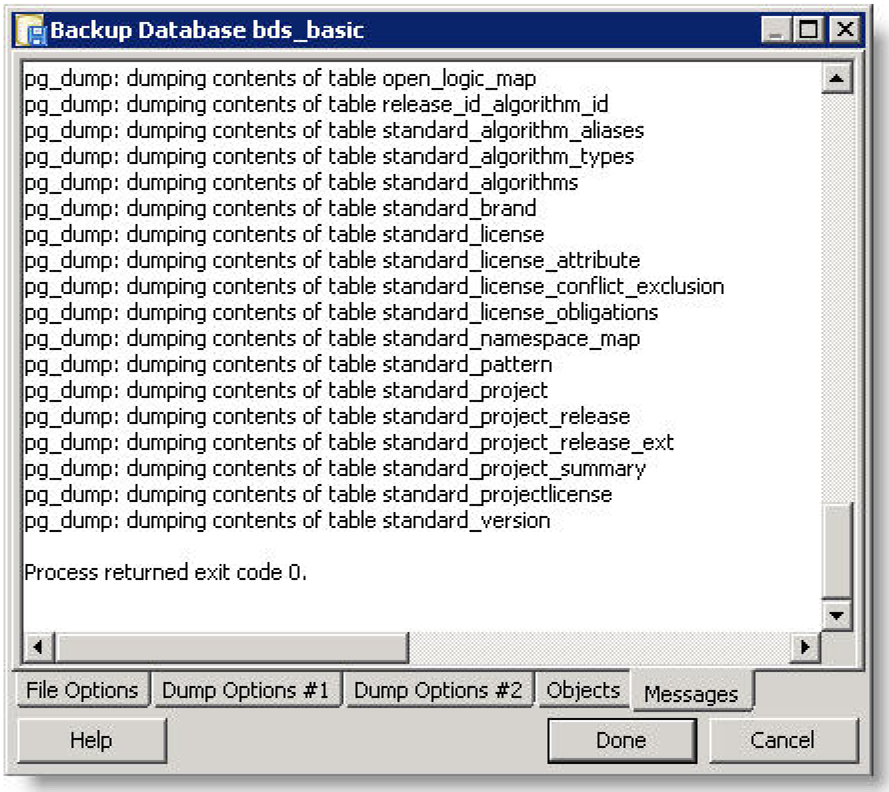
☑ Blobs
☐ With OIDs
☐ Insert commands
☐ Disable $ quoting

PLAIN options
☐ Only data
☐ Only schema
☐ No owner
☐ Create DB
☐ Drop DB
☐ Disable Trigger

☑ Verbose messages

9. When the process completes, click **Done**.

Figure 5.7: Backup complete message



```
pg_dump: dumping contents of table open_logic_map
pg_dump: dumping contents of table release_id_algorithm_id
pg_dump: dumping contents of table standard_algorithm_aliases
pg_dump: dumping contents of table standard_algorithm_types
pg_dump: dumping contents of table standard_algorithms
pg_dump: dumping contents of table standard_brand
pg_dump: dumping contents of table standard_license
pg_dump: dumping contents of table standard_license_attribute
pg_dump: dumping contents of table standard_license_conflict_exclusion
pg_dump: dumping contents of table standard_license_obligations
pg_dump: dumping contents of table standard_namespace_map
pg_dump: dumping contents of table standard_pattern
pg_dump: dumping contents of table standard_project
pg_dump: dumping contents of table standard_project_release
pg_dump: dumping contents of table standard_project_release_ext
pg_dump: dumping contents of table standard_project_summary
pg_dump: dumping contents of table standard_projectlicense
pg_dump: dumping contents of table standard_version

Process returned exit code 0.
```

10. Repeat steps 7-9 for each database listed in Protex Database Names on page 85, providing a unique name for each backup file.
11. Restart Tomcat.

5.2.4 Restoring the Database - Linux

The restore option lets you retrieve files you have backed up using the dump process. After saving your databases to a file, you can then restore a particular database if required.

✱ **To restore a damaged or corrupted database on Linux:**

1. Log in as root.
2. Change to the *bds-protexip* user, using the following command:

```
su - bds-protexip
```

3. Delete the original database using the following command:

```
dropdb bds_customer
```

4. Re-create the database using the following command:

```
createdb bds_customer
```

This creates a new database and provides output that shows *CREATE DATABASE*. If you make configuration modifications to improve performance, you may need to supply various options to *CREATE DATABASE* depending on your circumstances. Upon creation, you must upload your database with your data.

5. Issue the following command:

```
psql -c "grant all on database bds_customer to blackduck" template1
```

6. Drop the language because it is created as part of the restore:

```
droplang plpgsql bds_customer
```

7. To upload your database, use the following command:

```
pg_restore -d bds_customer bds_customer.dump
```

Note: Tomcat must be stopped for the `pg_restore` procedure.

Additionally, if you have a multi-core processor, you can increase the speed of the restoration by using the `-j` parameter to specify the number of parallel processors to use. Do not set this value higher than the number of available processors. For example:

```
pg_restore -j 4 -d bds_customer .dump
```

After this process is complete, you have successfully reverted to your old database.

Note: After restoring the database, you should rebuild the Solr index. For information, refer to Building a Solr Index on page 83.

5.2.5 Restoring the Database - Windows

The restore option lets you retrieve files you have backed up using the dump process. Once you have saved your databases to a file, you can then restore a particular database if required.

On a Windows system, you can use the **pgAdmin III** tool to restore your backup files. This is similar to the procedure for backing up your databases. To restore, the steps are:

- Drop the corrupted database.
- Create a new database.
- Restore the dump file into the new database.

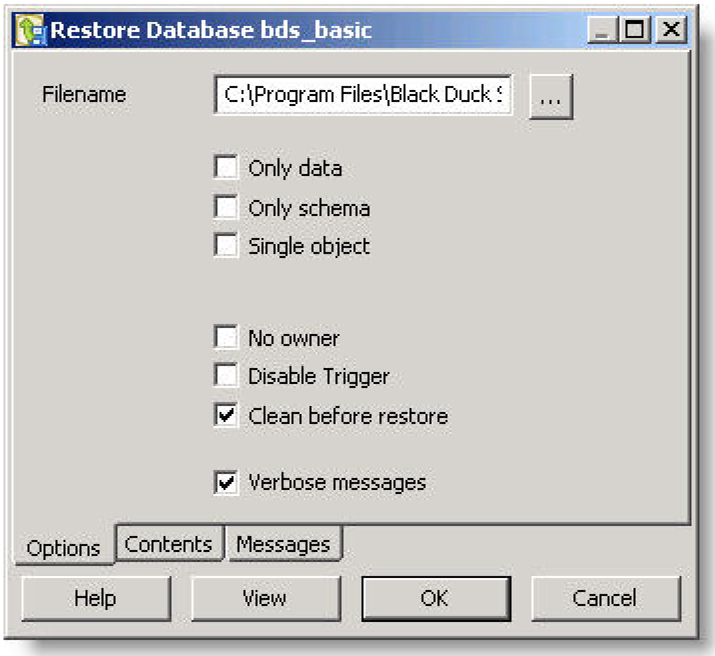
Another difference is that you can perform the backup as the *blackduck* user, but must create the new database as the *bds-protexip* user. Please contact Black Duck Customer Support for the *bds-protexip* password.

Note: As with backups, you must stop Tomcat during the restore process.

✱ To restore a damaged or corrupted database on Windows:

1. Connect to the database as when doing a backup. Use the *bds-protexip* user and the password you received from Black Duck Customer Support.
2. Select the option to restore into a clean database. This causes **pgAdmin** to first drop the old database before restoring the dump file. Alternately, you could drop the existing database and recreate it. If so, create the database as the owner of *bds-protexip*, set the template to *template1*, and grant *all* to user *blackduck*.

Figure 5.8: Restoring a Database on Windows



Restore Database bds_basic

Filename: C:\Program Files\Black Duck S

□ Only data
□ Only schema
□ Single object

□ No owner
□ Disable Trigger
☑ Clean before restore

☑ Verbose messages

3. Continue restoring the other database dump files.
4. Restart Tomcat.

Note: After you restore the database, you should re-build the Solr index. For instructions, see Building a Solr Index on page 83.

5.3 Managing Updates

Protex provides periodic updates that keep you current with the latest changes to the KnowledgeBase and the latest versions of the Protex software.

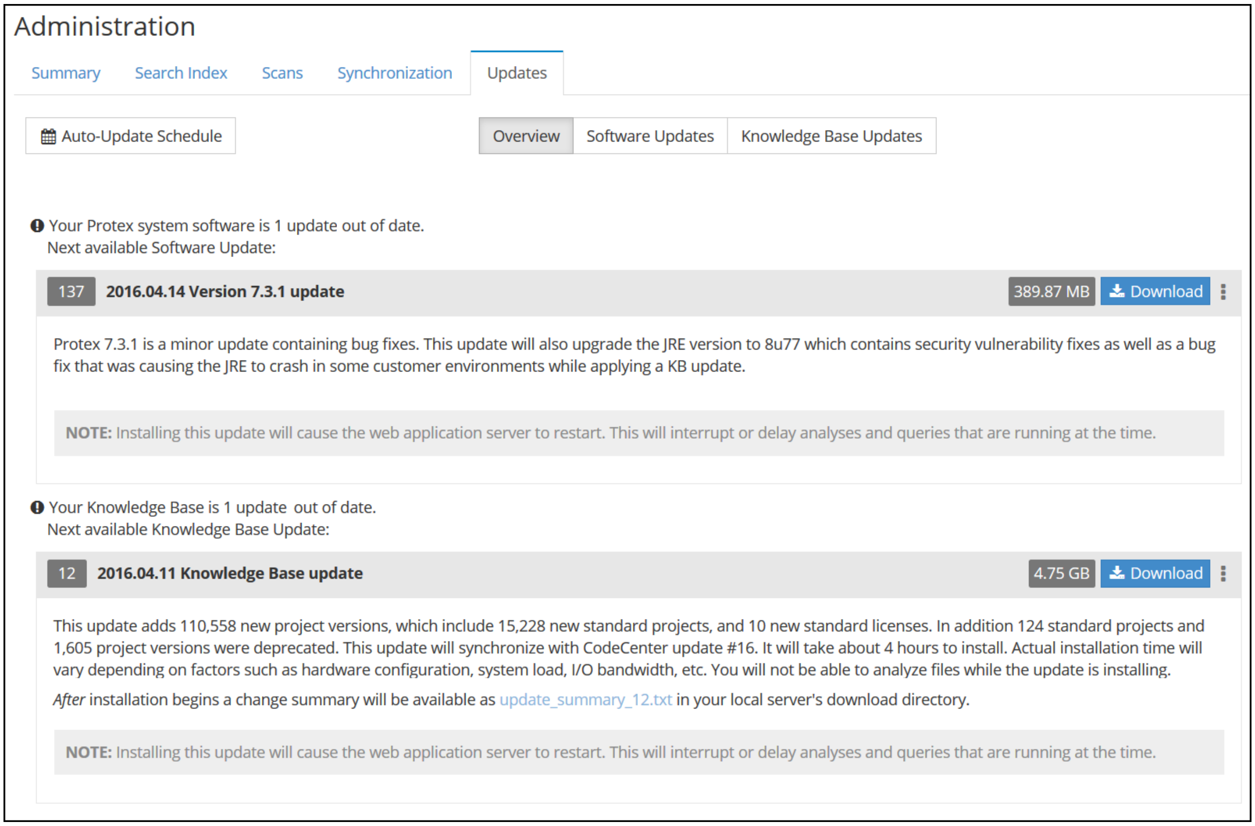
✱ To manage updates:

1. In the Classic user interface, click the Black Duck logo in the upper left corner to launch the Suite user interface.
2. In the Suite user interface, click the username drop-down menu.

3. In the username drop-down menu, click **Administration**.
4. On the **Administration** page, click **Updates**.
5. Use the **Updates** page to manage software and KnowledgeBase updates. This page enables you to:
   - Check your current update version.
   - Configure update options.
   - Specify the automatic updates schedule.
   - View a list of available updates.
   - Perform manual updates.

The **Updates** page provides settings enabling you to configure Protex to automatically download and install available updates.

Figure 5.9: Update Status Page showing Active Updates



Your Protex system software is 1 update out of date.
Next available Software Update:

137 **2016.04.14 Version 7.3.1 update** 389.87 MB Download

Protex 7.3.1 is a minor update containing bug fixes. This update will also upgrade the JRE version to 8u77 which contains security vulnerability fixes as well as a bug fix that was causing the JRE to crash in some customer environments while applying a KB update.

NOTE: Installing this update will cause the web application server to restart. This will interrupt or delay analyses and queries that are running at the time.

Your Knowledge Base is 1 update out of date.
Next available Knowledge Base Update:

12 **2016.04.11 Knowledge Base update** 4.75 GB Download

This update adds 110,558 new project versions, which include 15,228 new standard projects, and 10 new standard licenses. In addition 124 standard projects and 1,605 project versions were deprecated. This update will synchronize with CodeCenter update #16. It will take about 4 hours to install. Actual installation time will vary depending on factors such as hardware configuration, system load, I/O bandwidth, etc. You will not be able to analyze files while the update is installing.

After installation begins a change summary will be available as update_summary_12.txt in your local server's download directory.

NOTE: Installing this update will cause the web application server to restart. This will interrupt or delay analyses and queries that are running at the time.

For more information, refer to Automatic Updates on page 96 and Manual Updates on page 98.

Note: To perform an update, you must be an administrator.

Note: Some updates may perform an automatic restart of the Tomcat server.

Important: New code analysis is blocked during update installations. Existing jobs continue to run, although at a slower pace. At the end of the update, all jobs that have not finished are canceled. These jobs can be restarted and resume from the point at which they stopped.

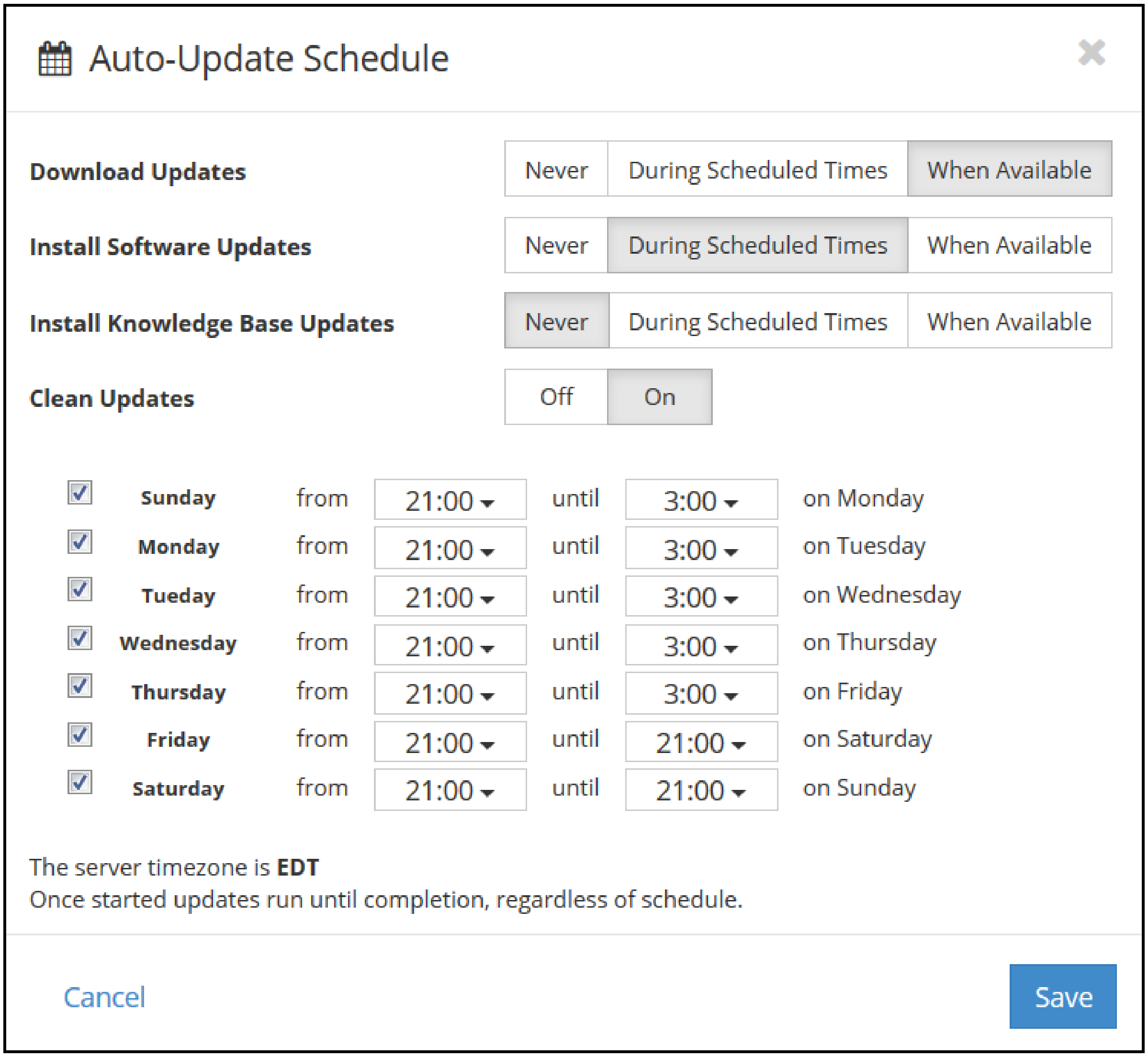
5.3.1 Automatic Updates

You can configure Protex to automatically download and install database updates, KnowledgeBase updates, and Protex software updates. Click **Auto-Update Schedule**, and choose one of the following for automatic downloading and updating:

- If your site does not have a dedicated Black Duck administrator, leave the default settings checked, and accept the updates as they occur. Protex installs the updates as soon as they are downloaded.
- If your site has a dedicated Black Duck administrator, and if you run lengthy code scanning and analysis cycles, the administrator might prefer not to configure automatic updates, but to manually update your Protex environment. It can be taxing on system resources to be running an installation procedure at the same time a lengthy code analysis procedure is underway.

✱ **To schedule automatic updates:**

1. Log in to Protex.
2. If you are in the Classic interface, click the Black Duck logo in the upper left corner to launch the Suite user interface.
3. From the user name menu in the **Suite** interface, select **Administration**.
4. On the **Administration** page, click **Updates**.
5. On the **Updates** page, click **Auto-Update Schedule**. The **Auto-Update Schedule** panel displays.



Auto-Update Schedule

Download Updates: Never | During Scheduled Times | [✓ When Available]

Install Software Updates: Never | [✓ During Scheduled Times] | When Available

Install Knowledge Base Updates: [✓ Never] | During Scheduled Times | When Available

Clean Updates: Off | [✓ On]

☑	Sunday	from	21:00	until	3:00	on Monday
☑	Monday	from	21:00	until	3:00	on Tuesday
☑	Tueday	from	21:00	until	3:00	on Wednesday
☑	Wednesday	from	21:00	until	3:00	on Thursday
☑	Thursday	from	21:00	until	3:00	on Friday
☑	Friday	from	21:00	until	21:00	on Saturday
☑	Saturday	from	21:00	until	21:00	on Sunday

The server timezone is **EDT**
Once started updates run until completion, regardless of schedule.

6. From the **Download Updates** menu, select **During Scheduled Times** or **When Available**. Select **Never** if you want to manually download and install updates.
7. From the **Install Software Updates** menu, select **During Scheduled Times** or **When Available**. Select **Never** if you want to manually download and install software updates.
8. From the **Install KnowledgeBase Updates** menu, select **During Scheduled Times** or **When Available**. Select **Never** if you want to manually download and install KnowledgeBase updates.

> **Note:** You should configure Protex to automatically download available updates and automatically install KnowledgeBase updates. However, we recommend that you manually perform software update installations.

9. If you want to clean up files after installation, select **On** from the **Clean Updates** menu.
10. In the day settings section, specify the schedule for your local Protex server to check for updates from Black Duck. If you specify a long duration, the Black Duck server is checked during that time

interval, and retries if the connection fails. If you select automatic downloads and installs, the system handles these actions appropriately.

Note: Once an update starts, it runs until is it complete, regardless of the duration you select.

11. Click **Save** .

Tip: Protex can send email to the system administrator after an automatic upgrade if their address is specified on the **Admin Center** > **Product Registration** page.

5.3.2 Manual Updates

Use the **Administration** > **Updates** page to perform manual (on-demand) updates of your Protex software, or to get the latest KnowledgeBase update.

✱ **To perform a manual update:**

1. Log in to Protex.
2. From the user name menu in the **Suite** interface, select **Administration**.
3. A message near the top of the page shows by how many versions your Protex software or KnowledgeBase is out of date.
4. Choose the download you want and click **Download**. The download size displays at the left of **Download**. The download begins, and the **Download** button changes to the download status percentage.
5.
6. After the download is complete, the **Download** button changes to an **Install** button.
7. Click **Install**. When the installation is complete, Protex displays a **Delete** link that lets you reclaim the disk space used for the download.
8. You can also click the three-dot button at the right of **Download**/**Install** to view the log files.

5.4 Administrator Audit Trail

Protex administrators (users who have permission to read configuration data) can run an administrator audit report on users who have modified functionality within Protex. The administrator audit report tracks all actions performed by administrator users: creating users, updating, deleting, and more. Administrator activities are available as a report, with a history date range of up to one year.

✱ **To create an administrator audit report:**

1. From the username menu in the Suite interface, select **Tools**.
2. In the Classic interface, select **Tools** > **Admin Center** > **Audit History**.
3. On the **Audit History** page, select the administrator users to appear in the report. You can select more than one. If you do not select a user or users, the report contains data from all administrator users.

4. On the **Audit History** page, select a date range using the **Select Period From** and **To** calendar selectors. You can specify a report history of up to one year.
5. Click **Download**.
6. You can save the report, or open it. The administrator audit trail report opens in the application configured for .CSV files. The report naming convention is `AdminAuditHistory-<date(time)>.csv`.
7. Columns in the audit trail report include:

- **Date** - The date of the event.
- **Originator** - The username executing the event.
- **Origin** - The IP address of the machine where the event was executed.
- **Trigger** - The section of Protex where the action originated: either the UI or SDK.
- **Section** - Area of Protex where the action originated; for example, the **Settings** section.
- **Event** - The action executed by the administrator; for example, create a new user.
- **Event Data Key** - Specifics of the event; for example, if the **Event** field shows a new user, this field displays the name of the new user. Note that user passwords are not captured in the report. If the **Event** field shows **Update Policy Manager General**, the value of **Event Data Key** may show **Options**.
- **Event Data Value** - Specific value for the event. For example, if an option was changed, this field displays the changed value. An example of an **Options** change is *Allow server file access = true*.
- **Event Result** - *Success* or *Fail*.
- **Event Result Reason** - If the value for **Event Result** is *Fail*, this field displays the reason for the failure.

Important: The following events are not captured in the administrator audit trail report:
– Invalid registration events
– Scan server administration
– Spring security synchronization

Chapter 6: Managing Users

User management within Protex involves the following tasks:

- Configuring Protex for self-registration
- Creating user accounts
- Assigning roles to users
- Assigning users to projects
- Removing users from projects
- Renaming user accounts
- Deleting users

6.1 Understanding User Roles

Protex has role-based rights and privileges. All Protex users must have at least one role assigned to their user account to use Protex.

Super User Role (Single-User Configurations)

Protex does not have a single role that confers super user privileges to all features and functions. If you want a single user to be able to access all Protex features, you must assign that user the following roles:

- Administrator
- Attorney
- Custom component manager
- Manager

(Black Duck) Administrator

The administrator has two areas of responsibility: technical infrastructure, and Protex system administration.

- Technical infrastructure: Procure server, install operating system, install Protex, create backup policies, manage server updates, test and troubleshoot connection issues.
- Protex system administration: Create users, assign roles, schedule and install updates, and set system defaults based on your policies.

You may have more than one administrator; an administrator from the IT Department might manage the technical infrastructure, while an administrator from engineering might manage the Protex system administration.

Only users with the administrator role can perform the following tasks:

- Register your Protex license key.
- Create user accounts.
- Assign roles to user accounts.
- Schedule Black Duck updates.
- Install Black Duck updates.

An administrator can also:

- Manage string searches at the global level using the **String Search Manager**.
- Set global policies for projects, including Rapid ID policies, using the **Policy Manager**.
- Teach identifications (if they also have the manager role).
- Download the Protex client software.

An administrator cannot perform the following tasks:

- Create projects or run analysis.
- Review and resolve analysis results.

Attorney

The attorney role is assigned to users responsible for assuring that your legal compliance requirements are met. The attorney role includes:

- Reviewing and approving component use at the project level. In some organizations, this responsibility is shared with or done by managers.
- Setting global policies for analysis.
- Administering the license management functionality in Protex.

In some organizations, attorneys play a day-to-day role in the Protex process; in others, they interact only with license management and other policy modules; and in others, they provide counsel and direction but do not use the system.

Only an attorney can:

- Create and manage custom licenses.
- Accept and prohibit licenses (approve/disapprove licenses).

An attorney can also:

- Run analysis.
- Review analysis results.
- Resolve issues.

An attorney cannot create a new project.

Note: This role was previously called license manager.

Custom Component Manager (formerly Code Print Manager)

You may choose to customize Protex by creating a catalog of custom components to track the reuse of code within your organization, or to add projects that are not already included in the standard KnowledgeBase (KB). You can assign a user the custom component manager role to carry out the work of creating code prints. This role should be tightly held, as custom components should be carefully controlled. This role is generally combined with a power developer or manager role.

- Only a custom component manager can create custom components. This role is generally used in conjunction with another role.

A custom component manager can also:

- Review analysis results.
- Resolve issues.

A custom component manager cannot create a new project or run analysis.

Note: This role was previously called code print manager.

Developer (formerly auditor)

The developer role is a limited role that is primarily used by applications and scripts to perform automated tasks. Assign the developer role to technical users whose responsibilities in Protex are solely at the project level.

A developer can:

- Run analysis from the command line.
- View the components in the KnowledgeBase through the **Component Manager** (read-only access).

A developer cannot:

- View the Bill of Materials or make identifications.
- View the **Review** tab.

Note: This role was previously called auditor.

Identification Only

These roles are designed for users whose only task is to perform identification work on Protex discoveries.

A user with one of these roles is only allowed to perform actions in the **Identify** area in the Classic user interface. These roles are restricted from performing any other action within Protex. They have read-only access to the following:

- Manage area in the Classic interface, so that they can view the path to the project code and the analysis settings.
- Review area in the Classic interface, so they can view approved and rejected components.

A user with the identification-only role cannot:

- View the **Reports** area.
- Make changes in the **Review** area.

Manager

Managers are technical users whose responsibilities span much of the Protex functionality. The key responsibilities of a manager are:

- Reviewing and approving of component use at the project level. In some organizations, this responsibility is shared with or done by attorneys.
- Designates a limited set of system policies, including analysis defaults and global approval of components.

In some organizations, the technical lead for the Protex system has dual roles; the manager role allows him to participate in project level analysis and review, while the administrator role allows him to manage users and system policies.

A manager can:

- Run analysis.
- Examine analysis results and resolve issues in the **Identify** tab.
- Make project assignments.
- Mark obligations as fulfilled.

Note: This role may also be called project manager.

Power Developer

Power developers are the day-to-day technical users of Protex. The people filling these roles come from engineering, IT, product management, and other areas closely connected to the development process.

Power developers are:

- Developers and others having intimate familiarity with the code are responsible for identifying Protex discoveries. This is the most time-consuming of the Protex processes.
- Release engineers or developers executing your automation and integration strategies.

A power developer can:

- Run analysis.
- Examine analysis results and perform identifications.

A power developer cannot create a new project.

Project Leader

A project leader has similar permissions to a power developer, with the added ability to create new projects.

A project leader can:

- Create a new project.
- Run analysis.
- Examine analysis results and perform identifications.

Read-Only

This role grants users read-only access to projects to which they have been assigned. They cannot perform actions or modify settings or data. This role supports workflows where you want to lock identifications during the review phase, but still allow the users who made the identifications to view their projects.

A user with this role has read-only access to:

- Project lists (Your Protex in the Suite user interface, My Protex area in the Classic interface).
- All project graphs and charts in the Suite user interface.
- **Manage** area in the Classic interface, to view project description, path to code, and analysis settings.
- **Identify** area in the Classic interface, to view discovered and identified components.
- **Review** area in the Classic interface, to view approved and rejected components.

Server Synchronization

This role is required if you have implemented a multi-server synchronization environment. Enabling multi-server synchronization locks settings and data for users that do not have this additional role. This role lets you control users that can modify data being synchronized. Users with this role may edit data to which they normally have access which is synchronized with other servers. Users without this role are able to view data that they have permissions to view, but cannot edit.

> **Note:** If you have not implemented a multi-server synchronization environment, you do not need to assign this role to users.

6.2 Protex User Role Matrix

Roles provide user privileges. The roles assigned to a Protex user account determine the tasks a user can perform. Every user should be assigned at least one role. You can assign multiple roles to a user if you want to give them multiple sets of privileges. The following table describes each role and its privileges.

Table 6.1: Protex User Roles

	Administration	Attorney	Custom Component Manager	Developer	Manager	Power Developer	Project Leader	Identification Only	Read–only	Server Synchronization
Select a project and view its status on the My Protex dashboard.		X	X		X	X	X	X	X	
Create a new project (using button in My Protex area).					X		X			
Clone a project (using **Manage** > **Project**).					X		X			
Edit project data, or delete file content (using **Manage** > **Project**).					X	X	X			
Delete a project (using button in My Protex area)					X					
Configure the parameters used during analysis (using **Manage** > **Settings**).					X	X	X			
Set the parameters for local Rapid ID configurations (using **Manage** > **Settings**).					X		X			
Analyze a project (start it with the button on **Manage** > **Analysis**). * Command line only.		X		X*	X	X	X			
Specify what kinds of matches will require identification.					X	X	X			
Create, edit, and delete local string searches and file patterns.		X	X		X	X	X			
Create users and assign roles.	X									
Assign users to project. Administrators can add users to any project. Managers and Project Leaders can add users only to projects to which they have access.	X				X		X			

	Administration	Attorney	Custom Component Manager	Developer	Manager	Power Developer	Project Leader	Identification Only	Read–only	Server Synchronization
Create obligations.	X	X								
Fulfill obligations.					X					
Create and edit licenses (using **Tools** > **License Manager**). Resolve license conflicts (using **Review** area).		X								
Identify or declare the components found in your project (**Identify** area).		X	X		X	X	X	X		
Use the **Run Rapid ID Now** feature.		X	X		X		X	X		
Set or change the approval status of a component (using the **Review** area).		X			X					
Generate reports for a project.		X	X		X	X	X			
Perform product registration and schedule online updates	X									
Download the Protex Client software.	X	X	X	X	X	X	X	X		
Create, edit, and delete global string searches (using **Tools** > **String Search Manager**)	X	X			X					
Set global policies for your projects, including Rapid ID policies (using **Tools** > **Policy Manager**)	X	X								
Edit access to component attributes, including creating custom components and patterns. Also, deleting custom components.			X							
Restore the original attributes to a modified component. * You must have both roles to perform this function.		X*	X*							
Have read access to the components in the KnowledgeBase (using **Tools** > **Component Manager**).	X	X	X	X	X	X	X	X	X	

	Administration	Attorney	Custom Component Manager	Developer	Manager	Power Developer	Project Leader	Identification Only	Read–only	Server Synchronization
Teach identifications for reuse in other projects. * You must have the manager role, plus one of the other indicated roles.	*	*			X*					
Grants the ability to modify settings and data that are synchronized in a multi-server synchronization implementation. * The user must first have a role that grants the ability to create or modify a setting or data. Enabling multi-server synchronization locks settings and data for users that do not also have this additional role.										X*

6.3 Adding a User

The **Tools** > **User Accounts** pages in the Classic interface let the Protex administrator add new user accounts to the system. Adding a new user is comprised of three steps:

1. Creating the user account.
2. Assigning one or more roles to the user account.
3. Assigning the user to one or more projects within Protex.

Roles provide user privileges to the Protex software. Every user must be assigned to at least one role. You can assign multiple roles to a user if you want to give them multiple sets of privileges. In addition, you must assign users to projects. Project assignments provide users access to data within Protex.

Note: Protex provides a default administrator login for the Protex Administrator.

Important: For users to perform tasks within Protex, you must ensure that you assign new users both roles and projects. Users without the administrator role cannot add themselves to a project.

✱ **To add a new user:**

1. Log in to Protex as an administrator or manager.
2. From the user name menu in the **Suite** interface, select **Administration**.
3. On the **Administration** > **Summary** page, click **User Accounts**.
4. In the Classic interface, on the **Tools** > **User Accounts** screen, click **Create User**. The **Create New User** dialog opens.
5. Enter the user's first and last names.
6. Enter the user's email address. Protex uses email addresses as the user names on accounts. The email address is case sensitive.
7. Enter the new password. The minimum password length is six characters.
8. Click **Save**.

Tip: Remember to assign roles and projects to the new user. For additional information on assigning projects, refer to Assigning Users to Projects on page 110

6.4 Assigning Roles to Users

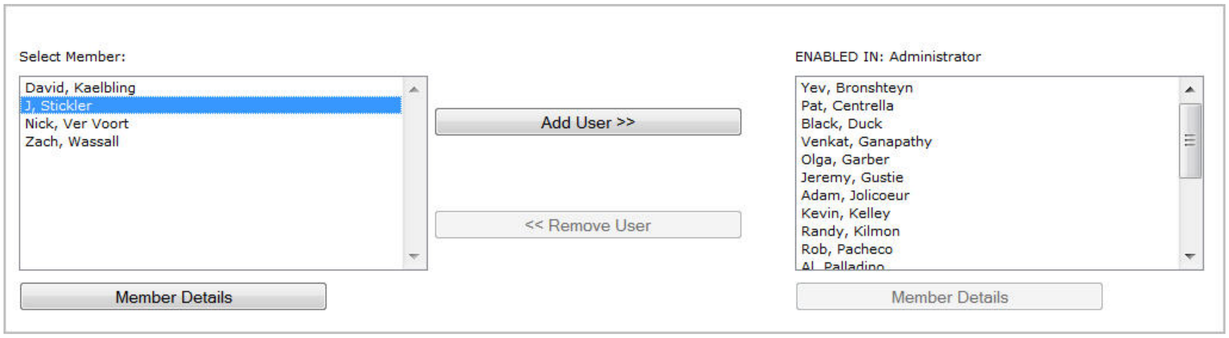
There are two methods for assigning roles to users. Both are described as follows; use the method that best fits your workflow and preferences.

Note: You must have the administrator role to perform this procedure.

✱ To add roles to a user on the User Role page:

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Users** > **User Roles**. The **User Role** page opens, displaying a list of roles:
    - Administrator
    - Attorney
    - Custom Component Manager
    - Developer
    - Identification Only
    - Manager
    - Power Developer
    - Project Leader
    - Read-Only
    - Server Synchronization
4. Click the role you want to assign to a user. The bottom of the screen refreshes to display a list of available users, and all users currently assigned to that role.

Figure 6.1: Tools > User Roles



Select Member:

David, Kaelbling
J, Stickler
Nick, Ver Voort
Zach, Wassall

ENABLED IN: Administrator

Yev, Bronshteyn
Pat, Centrella
Black, Duck
Venkat, Ganapathy
Olga, Garber
Jeremy, Gustie
Adam, Jolicoeur
Kevin, Kelley
Randy, Kilmon
Rob, Pacheco
Al, Palladino

5. From the **Select Member** list, highlight the user and click **Add User >>**.
6. Protex moves the user name to the **Enabled in** list.

✱ To add roles to a user on the User Accounts page:

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. a. In the Classic interface, select **Tools** > **Users** > **User Accounts**. The **User Accounts** page

opens, displaying a table of users.

4. On the **User Accounts** page, click a user name in the table. Protex displays additional information below the user name table.
5. In the lower half of the page, click the **Roles** tab.
6. In the **Roles** page, select the check box(es) for the additional roles to grant to the selected user.
7. Click **Save**.

Note: Users must also be assigned to projects. For additional information, refer to Assigning Users to Projects on page 110.

6.5 Assigning Users to Projects

Users can only view data and perform tasks for projects to which they have been assigned.

Users who are system administrators and managers can assign other users to a project. Administrators can add users to any project. Managers can add users only to projects to which they have access.

Note: Before adding a user to a project, you must first add the user to the system and assign them a role.

There are three ways you can assign a user to a project:

1. From the user account record (**Tools** > **User Accounts**). This method is preferable if you are adding a user to multiple projects.
2. From the project member management page (**Tools** > **Assign Project Members**). This method is preferable if you have created a new project and are assigning multiple users.
3. From the project page (**Manage** > **Users**). This method is useful if you are already working in the project and want to assign new users to it.

✱ To add a project to a user account:

1. Log in to Protex as administrator or manager.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Users** > **User Accounts**. The **Search Users** page opens, displaying a list of the current users.
4. Select the user you want to assign to projects. The **User Profile** page opens.
5. Click the **Projects** tab.
6. Click the check boxes for projects to which you want to assign the user.
7. Click **Save**.

The user must log out and back in for the change to take effect.

✱ To assign a user to a project:

1. Log in to Protex as administrator or manager.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Users** > **Assign Project Members**.
4. In the project table, select the project to which you want to assign the user.
5. In the **Select Member** list, select the user and click **Add User>>**. Protex adds the user to the project and moves their name to the **Enabled In** list.

6.6 Removing Users from Projects

Managers and system administrators can remove members from a project.

There are three ways you can remove a user's access to a project:

1. From the user account record (**Tools** > **User Accounts**).
2. From the project member management page (**Tools** > **Assign Project Members**).
3. From the project page (**Manage** > **Users**).

✱ To remove a project from a user account:

1. Log in to Protex as administrator or manager.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **User Accounts**. The **Search Users** page opens, showing a list of the current users.
4. Select the user you want to remove from your project. The **User Profile** page opens.
5. Click the **Projects** tab.
6. Clear the check boxes for the projects from which you want to remove the user.
7. Click **Save**.

The user must log out and back in for the change to take effect.

✱ To remove a user from a project:

1. Log in to Protex as administrator or manager.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Assign Project Members**.
4. Select the project that you want to modify from the list.
5. In the **Enabled In** list, select the user you want to remove from your project and click the **<<Remove User** button. The user is removed from the project and moved to the **Select Member** list.

✱ **To remove a user from a project:**

1. Log in to Protex as administrator or manager.
2. From the username menu in the Suite interface, select **Tools**.
3. Click the **My Protex** link in the header.
4. Select the project from the list.
5. On the **Manage** page, click the **Users** tab.
6. In the **Enabled In** list, select the user you want to remove from your project and click the **<<Remove User** button. The user is removed from the project and moved to the **Select Member** list.

6.7 Removing Roles from Users

Note: You must have the administrator role to perform this procedure.

✱ **To remove roles from a user:**

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **User Accounts**.
4. Search for the user whose profile you want to modify.
5. In the lower half of the page, click the **Roles** tab.
6. Clear the check box for any role that you want to remove.
7. Click **Save**.

6.8 Renaming a User Account

The user name (based on the user's email) cannot be changed directly. However, you can create a new account with a new name and transfer all of a user's projects and roles to that new account.

When you transfer an account, the user's profile, including their roles and project memberships, are transferred to the new user and the old user profile is deleted.

✱ **To rename a user account, change the email address, or change the password associated with an account:**

1. Log in as administrator.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **User Accounts**. The **User Accounts** page opens.
4. In the user list, select the name of the user you want to transfer. The user's profile displays in the lower half of the page.
5. On the **General** tab, click the **Transfer Profile** button. The **Transfer User Profile** dialog box

opens.

6. **First Name**: Enter the user's first name.
7. **Last Name**: Enter the user's last name.
8. **E-mail**: Enter the user's email address. Protex uses email addresses as the user names on accounts. The email address is case sensitive.
9. **Password**: Enter the new password. The minimum password length is 6 characters.
10. **Verify Password**: Enter the new password a second time to verify it.
11. Click **Save**. The **User Accounts** page displays the new user.

6.9 Deleting a User

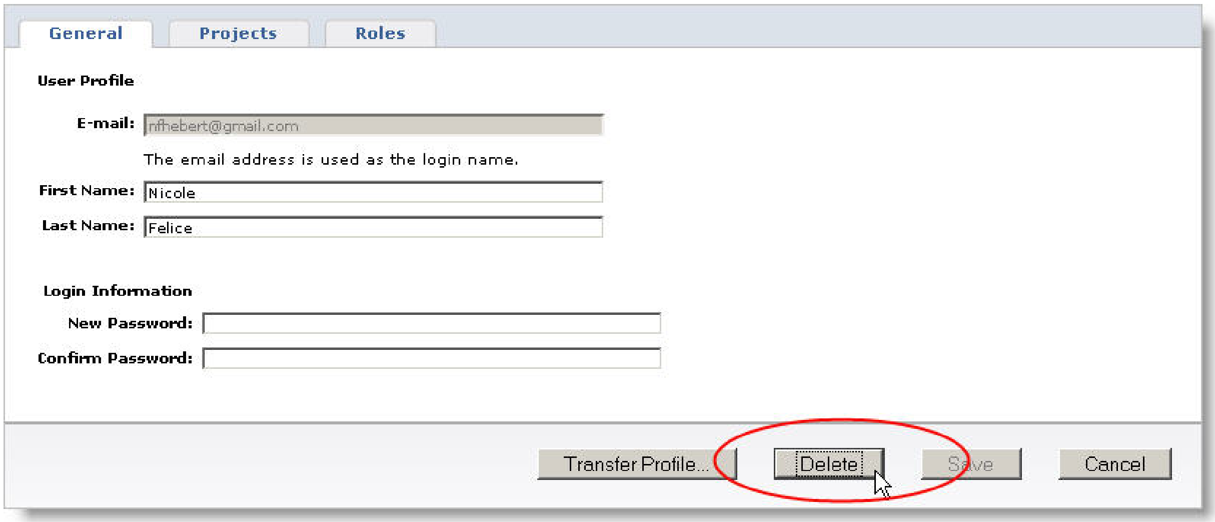
The system administrator has permission to delete users as long as they are not associated with projects.

Before deleting a user, remove them from all projects as described in Removing Users from Projects.

✱ To delete a user:

1. Log in to Protex as administrator or manager.
2. From the user name menu in the **Suite** interface, select **Administration**.
3. On the **Administration** > **Summary** page, click **User Accounts**.
4. In the Classic interface, on the **Tools** > **User Accounts** screen, select the user you want to delete. You can either search for the user, or use the Prev/Next links to navigate pages in the list. Selecting a user displays the user details in the lower half of the page.
5. Select the **General** tab.

Figure 6.2: Delete a User



E-mail: nfhebert@gmail.com

The email address is used as the login name.

First Name: Nicole

Last Name: Felice

6. Click **Delete**.

Chapter 7: Troubleshooting Protex

This chapter includes information to help troubleshoot your Protex environment, and Black Duck Support contact information.

7.1 Protex Log Files

Protex log files track the progress of many functions, including commonly scheduled tasks such as downloading and installing updates. Reviewing the log files may help you in troubleshooting issues. You may want to view the log files before contacting Black Duck Customer Support. Customer Support may also request copies of your log files to assist in troubleshooting issues.

You can view a variety of log files from the classic user interface by going to **Tools** > **Admin Center** > **View Logs**. Use the **Search** feature to select a specific log or to point to a specific directory path of logs. You can also use the **Show** filter to view a specific type of log file. Options in the **Show:** filter are:

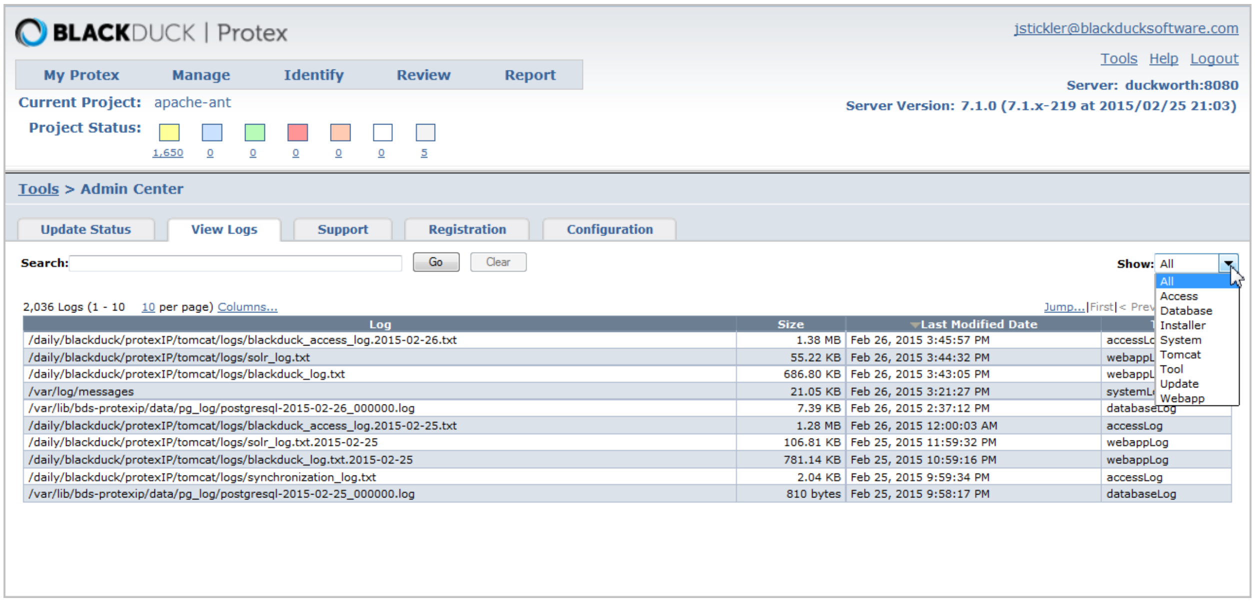
- **All** — Shows all log files available.
- **Access** — Lists all access logs.
- **Database** — Displays log files associated with the database in use.
- **Installer** — Displays all installation log files.
- **System** — Displays all system-related log files.
- **Tomcat** — Displays only Tomcat-related logs.
- **Tool** — Lists any tool-related log files.
- **Update** — Lists all update logs.
- **Webapp** — Displays all log files.

To view the complete log file, click an entry in the log file table. The complete log file opens in a new tab or a new browser window, depending on your browser settings. Additional project information is available from **Reports** > **Analysis Logs**.

7.1.1 Viewing Log Files

You can view log files from the Protex user interface.

Figure 7.1: Tools > Admin Center > View Logs tab



Server: duckworth:8080

Server Version: 7.1.0 (7.1.x-219 at 2015/02/25 21:03)

Current Project: apache-ant

Project Status: 1,650 0 0 0 0 0 5

2,036 Logs (1 - 10 10 per page) Columns...

Log	Size	Last Modified Date	T
/daily/blackduck/protexIP/tomcat/logs/blackduck_access_log.2015-02-26.txt	1.38 MB	Feb 26, 2015 3:45:57 PM	accessLo
/daily/blackduck/protexIP/tomcat/logs/solr_log.txt	55.22 KB	Feb 26, 2015 3:44:32 PM	webappL
/daily/blackduck/protexIP/tomcat/logs/blackduck_log.txt	686.80 KB	Feb 26, 2015 3:43:05 PM	webappL
/var/log/messages	21.05 KB	Feb 26, 2015 3:21:27 PM	systemL
/var/lib/bds-protexip/data/pg_log/postgresql-2015-02-26_000000.log	7.39 KB	Feb 26, 2015 2:37:12 PM	databaseLog
/daily/blackduck/protexIP/tomcat/logs/blackduck_access_log.2015-02-25.txt	1.28 MB	Feb 26, 2015 12:00:03 AM	accessLog
/daily/blackduck/protexIP/tomcat/logs/solr_log.txt.2015-02-25	106.81 KB	Feb 25, 2015 11:59:32 PM	webappLog
/daily/blackduck/protexIP/tomcat/logs/blackduck_log.txt.2015-02-25	781.14 KB	Feb 25, 2015 10:59:16 PM	webappLog
/daily/blackduck/protexIP/tomcat/logs/synchronization_log.txt	2.04 KB	Feb 25, 2015 9:59:34 PM	accessLog
/var/lib/bds-protexip/data/pg_log/postgresql-2015-02-25_000000.log	810 bytes	Feb 25, 2015 9:58:17 PM	databaseLog

Note that you can filter the log files displayed on the page using the **Show:** menu.

✱ To view a log file for your server:

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Admin Center**.
4. Click the **View Logs** tab. The **View Logs** page opens.
    - If you are looking for the cause of a recent change in behavior, sort the list by date.
    - If you are looking for a specific log file, select the appropriate type from the **Show** menu:
        - **Access**
        - **Database**
        - **Installer**
        - **System**
        - **Tomcat**
        - **Tool**
        - **Update**
        - **Webapp**
    - To search for a specific log entry, enter the word or phrase to locate in the **Search** field, and click **Go**. For example, enter *daily* to locate logs containing that word.
5. Select a log from the list. A new window opens and displays the contents of the log.

7.1.2 Linux Log Files

If you cannot access the Protex application, you can still directly access the log files using the file system. The log files may help you resolve your problem. If not, have a copy of them ready before you contact Black Duck customer support.

The following table summarizes the Protex log files and their default locations:

Table 7.1: Linux Log Files

Type	Path
Server installation logs	/tmp/Black_Duck_Protex_Install_<*date*>.log
	/tmp/installer_debug.txt
	/tmp/Protex_Install_<*date*>.log
	/tmp/BDS_IACA_Protex_server.log
Tomcat server logs	/opt/blackduck/protexIP/tomcat/logs/catalina.out /opt/blackduck/protexIP/tomcat/logs/catalina.<*date*>.out
API logs	/opt/blackduck/protexIP/tomcat/logs/api_log
Protex server	/opt/blackduck/protexIP/tomcat/logs/blackduck_log.txt.<*date*> /opt/blackduck/protexIP/tomcat/logs/api_log.txt
Protex access logs	/opt/blackduck/protexIP/tomcat/logs/blackduck_access_log.<*date*>.txt
Solr	/opt/blackduck/protexIP/tomcat/logs/blackduck_solr_access_log.<*date*>.txt /opt/blackduck/protexIP/tomcat/logs/solr_log.<*date*>.txt
Start-up configuration	/etc/sysconfig/bds_protexIP-tomcat (memory management) /opt/blackduck/protexIP/config/bds-protexIP-tomcat.start
Server synchronization	/opt/blackduck/protexIP/tomcat/logs/synchronization_log
Client install log	/tmp/Black_Duck_protexIP_client_installLog.log /tmp/Black_Duck_Protex_Client_Install_<*date*>.log
Client tool log	/home/<*user*>/.bdstool.log (.bdstool log file)
Protex client log	/tmp/protexIPClient.portnumber[.username]/logs

Within the Linux Protex log files, there are two log files requiring further explanation:

- `/tmp/BDS_IACA_Protex_server.log` — This file is built sequentially. It contains the action log output for the following:
  - Starting and stopping PostgreSQL.
  - Disk space checks.

  - Loading of dump files into PostgreSQL.
  - Migration of schema into PostgreSQL.

- `/tmp/installer_debug.txt` — This file is created and written at the end of the installation process. It contains the content of the `InstallAnywhere` variables. They include:
  - The logs of the Tomcat startup, including:

```
INSTALL_TOMCAT, INSTALL_STDOUT, INSTALL_STDERR, INSTALL_ERRORCODE.
```

  - The logs of the PostgreSQL initial installation, including:

```
INSTALL_POSTGRESQL_STDOUT, INSTALL_POSTGRESQL_STDERR, INSTALL_POSTGRESQL_
EXITCODE.
```

Tip: To find a variable, search these files using this syntax:

```
Property Name = <Value>.
```

7.1.3 Windows Log Files

On non-Windows 7 machines, your Protex log files reside in the following location:

```
C:\Documents and Settings\username\local settings\Temp
```

On Windows 7, the files are in:

```
C:\<username>\AppData\Local\Temp
```

The following table summarizes the Protex log files and their default locations:

Table 7.2: Windows Log Files

Type	Path
Server Installation logs	`C:\Users\<user>\AppData\Local\Temp\Black_Duck_Protex_Install_<date>.log`
	`C:\Users\<user>\AppData\Local\Temp\installer_debug.txt`
	`C:\Protex_Install_<date>.log`
	`C:\Users\<user>\AppData\Local\Temp\BDS_IACA_Protex_server.log`
Tomcat Server logs	`C:\Program Files\Black Duck Software\protexIP\tomcat\logs\catalina.<date>.txt`

Protex Server	`C:\Program Files\Black Duck Software\protexIP\tomcat\logs\blackduck_log.txt.<date>`
	`C:\Program Files\Black Duck Software\protexIP\tomcat\logs\api_log.txt`

Protex access logs	`C:\Program Files\Black Duck Software\protexIP\tomcat\logs\blackduck_access_log.<date>.txt`

Type	Path

Solr	`C:\Program Files\Black Duck Software\protexIP\tomcat\logs\blackduck_solr_access_log.<date>.txt`
	`C:\Program Files\Black Duck Software\protexIP\tomcat\logs\solr_log.txt.<date>`

Server Synchronization	`C:\Program Files\Black Duck Software\protexIP\tomcat\log\synchronization_log`

Protex Client log	`C:\Documents and Settings\<USER>\LocalSettings\Temp\protexIP.9000\logs\tomcat_log.txt (on Windows)`
	`C:\Users\<USER>\AppData\Local\Temp\protexIP.9000\logs\tomcat_log.txt (on Windows 7 and Vista)`

7.2 Memory issues with large projects

Both **bdstool** and the Protex Client may run out of memory when processing very large projects. Possible errors are `java.lang.OutOfMemoryError` or `java.lang.reflect.InvocationTargetException`. Should this occur, refer to Configuring Memory Options on page 76

Tip: If you plan to scan large projects, you should install the 64-bit version of the Protex client because it can handle larger memory settings. Due to Java limitations, the 32-bit version of the Protex client is restricted to 2GB of memory.

Note that minimum product system requirements are documented for small, medium, and large installations. Refer to the *Protex Installation Guide* for details.

7.3 HTTP Status 500 - Internal Server Error

Two common causes of this error message are:

1. Tomcat didn't shutdown properly during an upgrade.
2. Tomcat is running out of memory, often during the final license analysis step after all files have been analyzed.

Try editing the JAVA_OPTS line in `/opt/blackduck/protexIP/config` on the server to give the web server more memory, restart Tomcat, and try again.

7.4 System Error

These are generic errors reported when Protex detects an internal inconsistency or severe failure.

- Fingerprint match resulted in invalid list; possible `IOException`.

The most common cause for this error is **bdstool** losing communication with the local Protex server while analyzing files. Determine if the server needs to be restarted.

- Issue list limited by removal of ... Inserted Code issues

The project or file generated so many issues that tracking them would severely degrade performance. All issues are reported when generated and can be viewed, but they are not uploaded or saved for future analysis.

7.5 "Server redirected too many times (#)" when activating registration

Check that you have the correct proxy username and password. Some proxy servers return a redirect directive rather than an authentication failure status when they detect a problem, leading to message loops and the *Server redirected too many times (#)* error message.

7.6 File comparison issues

The following are known issues with the File Comparison tool.

- Due to licensing restrictions, source code for some projects in the KnowledgeBase that fall under a proprietary or otherwise restrictive license may not be available for file comparison. This is a small fraction of the over one million projects from the thousands of sites available in the KnowledgeBase.

In this case, Protex reports *no source code available*.

- Another case where the source code only appears to be unavailable is when using a proxy for the Protex server to access itself. In this case, you might also receive an HTTP 503 response code. The problem occurs when the proxy tries to find the file and fails at some point, and this information becomes stored in a cache. A workaround is to add the fully qualified domain name to the proxy exception list so that the system is reached directly instead of through the proxy. For example, edit the `/opt/blackduck/protexIP/config/bds-protexIP-tomcat.start` file and add the following to `http.nonProxyHosts` in the JAVA_OPTS section: `mysystem.bigcompany.com|localhost|127.0.0.1`.

> **Note:** On Windows, the Tomcat startup settings are configured in the following Windows Registry key:
>
> ```
> HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software
> Foundation\Procrun 2.0\protextc\Parameters\Java\
> ```

7.7 Workarounds When Using the File Comparison Feature

The following are known issues with the File Comparison tool.

- If the comparison pane cannot retrieve the source code for a matched project from the master server, or if your company prefers to not use this method, you can download and unpack a project's source code to a special location on your local server. You and others in your company can then easily access this source code for future review of code matches.

For easiest use, download and unpack the code into `/opt/blackduck/protexIP/source/<project-id>` on your local server. To determine this `<project_id>`, select the matched project under the **KB Project** left navigation area and look for the property called **Project Identifier** under the profile tab. Try to get the exact version of the project listed in the project profile of the project, and remove any symlinks. Finally, update the project location under the **Location** tab.

- Due to licensing restrictions, source code for projects that fall under a proprietary or otherwise restrictive license may not be available for file comparison. This is a small fraction of the over one million projects from the thousands of sites available in the KnowledgeBase.

In this case, Protex reports *No source code available*.

- Another case where the source code only appears to be unavailable is when using a proxy for the Protex server to access itself. In this case, you might also receive an HTTP 503 response code. The problem occurs when the proxy fails to find the file (perhaps before it is available), and this information becomes stored in a cache. A workaround is to add the fully qualified domain name to the proxy exception list so that the system is reached directly instead of through the proxy. For example, edit the `/opt/blackduck/bds-protexIP-tomcat` file and add the following to `http.nonProxyHosts` in the `JAVA_OPTS` section:

```
myprotexserver.bigcompany.com|localhost|127.0.0.1
```

7.8 Retry limit for Protex client

By default, a Protex client retries a command twice before aborting with a network timeout error similar to *Connection reset by peer*.

This retry setting is configurable. Setting this number higher can be helpful where the network reliability is not certain, or when the client has a consistent history of network disconnects.

The property that handles the retry attempts is:
`blackduck.axis.retry.exception.java.net.ConnectException=NumberofRetries`

Setting this property to `10` tells the client to make 10 attempts on a network error before giving up.

Add the following line to the `Client.properties` file under `C:\ProgramFiles\Black Duck Software\protexIP\config`, as follows:

```
blackduck.axis.retry.exception.java.net.ConnectException=10
```

Also note that if you have problems connecting using a short name, try using full names. For example, use `tank.blackducksoftware.com` instead of just the link name *tank*.

7.9 Highlighting of regex string search hits

When Protex finds a string search match, it shows the matching text highlighted in yellow. There is an issue with regex searches containing capture groups, where only the part of the matching text in the capture group is highlighted. For example, if you wanted to find the words *author*, *authored*, and *authors*, you could create a search for *author(ed|s).* Protex locates the desired words, but only highlights the text from the group (*ed* and *s*). A workaround is to search for each of the variations using the full words (*authored|authors|author*). Another option is to use non-capturing groups: *author(?:ed|s)*.

7.10 Performance issues on Red Hat Enterprise Linux 6.3

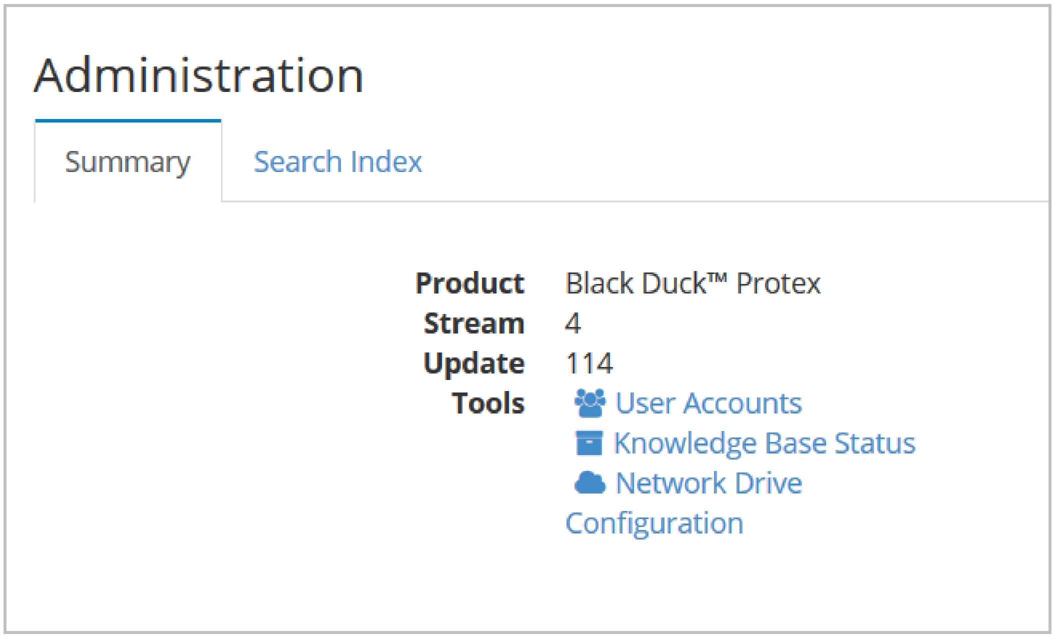
We have become aware of a performance issue with the NFS client in Red Hat Enterprise Linux 6.3. This can degrade your Protex performance, due to the effect on high PostgreSQL loads. If you cannot fully upgrade to RHEL 6.4, a workaround is to upgrade your kernel to the RHEL 6.4 kernel, while still running a 6.3 user environment.

7.11 Viewing Your Currently Installed Software and KnowledgeBase Version

The Black Duck KnowledgeBase (KB) of open source components is regularly updated with new and updated information. The Protex software is regularly updated with new features and bug fixes. The Protex Administration screens let you view the currently installed versions of the software and KnowledgeBase, and to manage your update schedule.

Tip: Before contacting Black Duck Support, check your currently installed versions, as you will be asked for this information.

Figure 7.2: Administration > Summary page - Suite interface



Administration

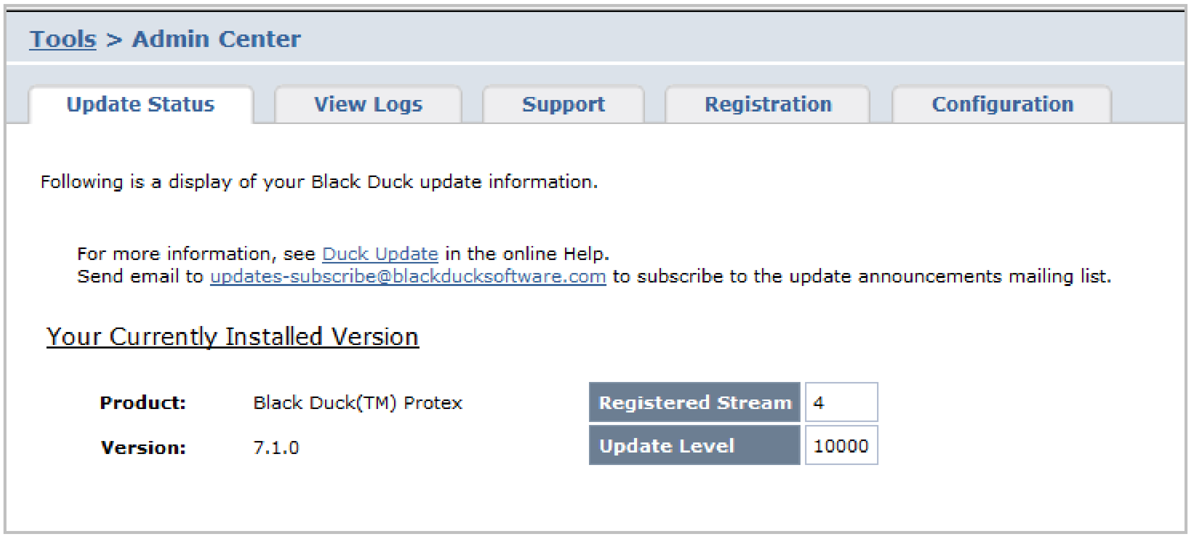
Product	Black Duck™ Protex
Stream	4
Update	114
Tools	User Accounts Knowledge Base Status Network Drive Configuration

✱ To view your installed versions in the Suite interface:

1. Log in to Protex.
2. From the user name menu in the **Suite** interface, select **Administration**. Protex displays the **Administration Summary** page.

Note: To schedule and manage updates, you must use the Classic interface.

Figure 7.3: Update Status Page - Classic Interface



Following is a display of your Black Duck update information.

For more information, see Duck Update in the online Help.
Send email to updates-subscribe@blackducksoftware.com to subscribe to the update announcements mailing list.

Your Currently Installed Version

Product:	Black Duck(TM) Protex	**Registered Stream**	4
Version:	7.1.0	**Update Level**	10000

✱ To view your installed versions in the Classic interface:

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **Admin Center**. The **Update Status** page opens.

Customer Support

If you have problems with the software or the documentation, please contact Black Duck Customer Support.

For complete customer service options, refer to:

https://www.blackducksoftware.com/support/contact-support

You can contact Black Duck Support in several ways:

- From within Protex: **Tools** > **Admin Center Support**
- Online: http://customerhub.blackducksoftware.com
- Email: support@blackducksoftware.com
- Phone: +1 781.891.5100, ext. 5

- Fax: +1 781.891.5145
- Hours: Monday - Friday 8:00 - 18:00 Eastern Standard Time (US EST)

Note: Customers with an Enhanced Customer Support Plan can contact customer support 24 hours a day, 7 days a week to obtain Tier 1 support.

To access a range of informational resources, services and support, as well as access to Black Duck experts, visit the Black Duck Customer Success Portal at:

https://www2.blackducksoftware.com/support/customer-success

You can use the Internet to log Protex issues. To use this resource, a login and password are required. Login credentials for this service are emailed to you at registration. However, if you have not received this information, or you have misplaced or forgotten your password, please contact Black Duck Customer Support.

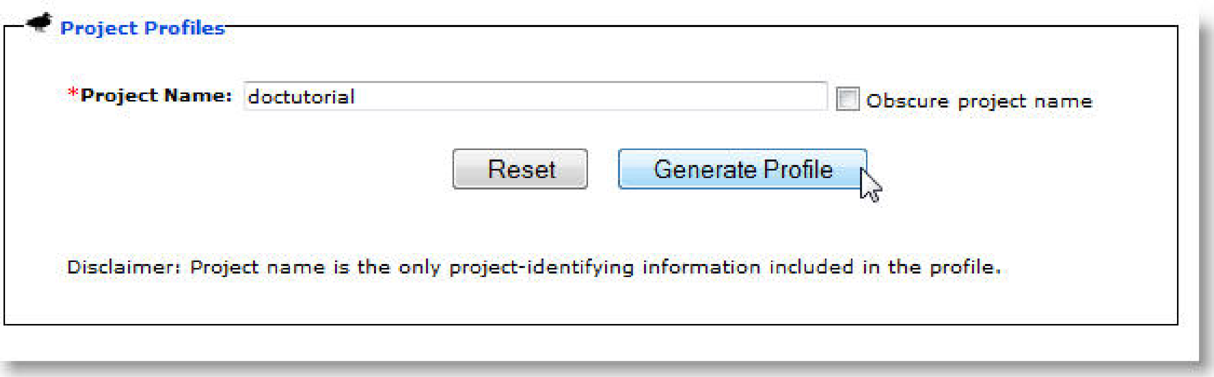
If you would like someone to perform Protex tasks for you, please contact the Black Duck Services group. They offer a full range of services, from planning, to implementation, to analysis. They also offer a variety of training options on all Black Duck products. Refer to https://www.blackducksoftware.com/services/ for more information.

7.11.1 Use the Project Profiler to Provide Additional Information

Protex includes a Project Profiler utility to help Black Duck recreate and debug issues encountered with your projects. The tool creates a statistical profile of a project so that a similar project can be recreated on our test systems. For example, the profile might indicate that your project has one thousand files (including 10 jar files), and one million discoveries. This information may help our engineers to recreate the problem without needing a database dump file.

The profiling system is accessed by navigating to `http://<ProtexServer>/protex/projectprofile`. If you are not already logged in, you are redirected to a login page. You can create a profile for any project for which you have access.

Figure 7.4: Project Profile Generation


Project Profiles

*Project Name: doctutorial

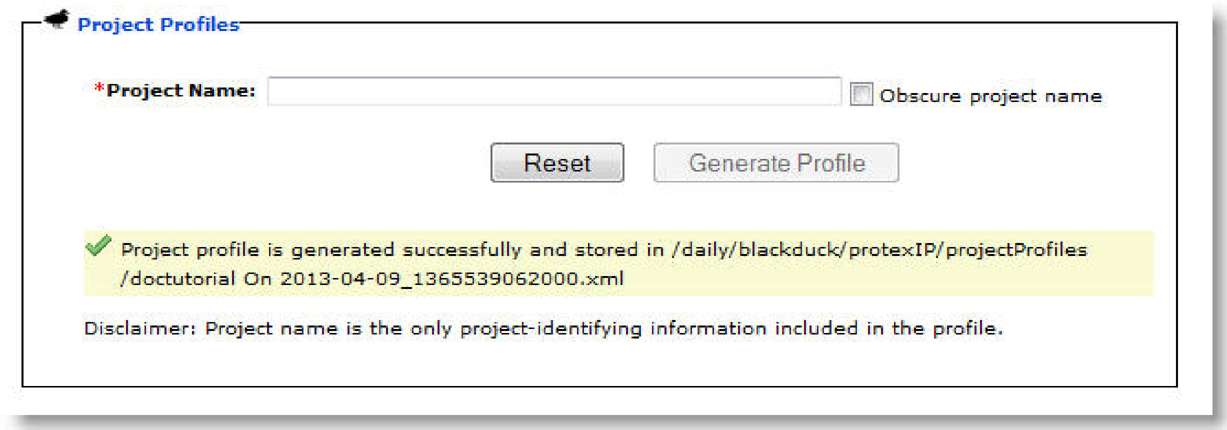
□ Obscure project name

Disclaimer: Project name is the only project-identifying information included in the profile.

The only identifying data gathered is the project name, which can be obscured by a hash function if desired.

Once the profiling operation completes, the location of the generated profile XML file displays. This file can then be sent to Black Duck Customer Support along with other details of the problem.

Figure 7.5: Project Profile Location



Project Profiles

*Project Name: □ Obscure project name

✓ Project profile is generated successfully and stored in /daily/blackduck/protexIP/projectProfiles /doctutorial On 2013-04-09_1365539062000.xml

Disclaimer: Project name is the only project-identifying information included in the profile.

7.11.2 Requesting License or Component Updates to the KnowledgeBase

There are three ways to request changes in the KnowledgeBase.

Using Email

You can request KnowledgeBase (KB) changes or report errors using email. Direct your correspondence to the following address:

```
knowledgebase@blackducksoftware.com
```

Using the Customer Support Login

You can also request KnowledgeBase changes using the Internet.

1. Log in to your customer support account as described in Logging Cases with Customer Support on page 125.
2. Select **Open Case** from the **Case Management** menu.
3. Change the **Case Type** to **KnowledgeBase Request**.
4. Enter the relative details and describe exactly what is wrong.

Using the Product

You can request KnowledgeBase changes from within Protex.

✱ To email Black Duck about a specific license or component:

1. Log in to Protex.
2. From the username menu in the Suite interface, select **Tools**.
3. In the Classic interface, select **Tools** > **License Manger** or **Tools** > **Component Manager**.

4. Select a license or component from the list. Protex displays the **General** tab at the bottom of the page.
5. Locate and click the **Email Black Duck about this license** or **EMail Black Duck about this component** link. You may need to scroll before the link is visible. Your email editor opens.
6. In the **Subject** field of the message, enter the name of your project.
7. In the message section, enter the details about the specified license or component. Include as much information as possible. This could include the following:
    - Component name.
    - License name.
    - Home page.
    - Where to add the component.
    - Contact information (Phone number, alternate email address, and so on).
8. Click **Send** to begin the request process. You are notified upon receipt of the request.
9. Click **Send** to complete the information request.

The new license or component will be researched, indexed, and added to a future update.

You can add local components to your database at any time using **Create Local Component**. For more information, refer to Creating a Local Component.

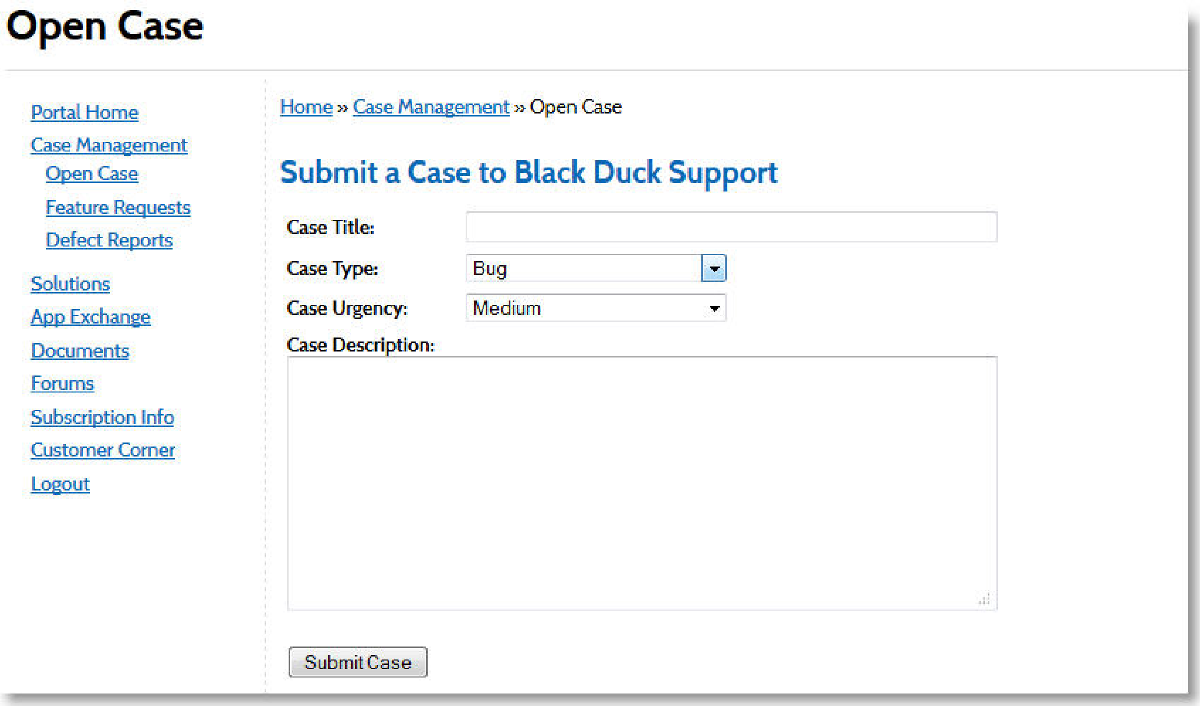
7.11.3 Logging Cases with Customer Support

If you are having support issues, you can contact the support team directly, or use the online customer portal to open a case. The Black Duck Customer Portal is available 24 hours a day, seven days a week.

In order to use the Customer Portal, you need a login and password, provided by Black Duck Software. Login credentials for this service are emailed to you at registration. However, if you have not received this information, or you have misplaced or forgotten your password, please contact Black Duck Customer Support using one of the methods listed in the Customer Support topic.

1. Login to the customer portal at: http://customerhub.blackducksoftware.com.
2. Before opening a new case, please check the **Solutions** area for fixes and workarounds to known issues.
3. Within the Support site, click **Case Management** > **Open Case** to open a new form.
4. Give a clear description about the problem. Please be as specific as possible and include your operating system, browser version, and Protex update level. You can attach log files and screen captures after submitting the ticket.
5. Click **Submit Case** to enter the case.

Figure 7.6: Open a Support Case



Submit a Case to Black Duck Support

Case Title:	
Case Type:	Bug
Case Urgency:	Medium
Case Description:	

After logging your case, you will receive a prompt response from the Black Duck Customer Support Team. You can use the **Case Management** area to keep up-to-date on the status of the problem you reported.

Appendix A: Data Gathered by Protex

Communication between customer site installation and Black Duck servers are described in the following sections.

A.1 Black Duck Network Components

The Black Duck network contains the following components:

- Registration server — Used to register and maintain all registration information.
- Update server — Provides periodic updates to customers.
- KnowledgeBase server — Used to authenticate projects and licenses.

Protex interacts with servers managed by Black Duck and hosted at secure data centers. Black Duck recognizes that Protex is being used in conjunction with valuable intellectual property. Black Duck treats the Internet-based communications between a customer installation of Protex and the data center servers as confidential information as described in Black Duck's agreement.

Note: To use the file comparison tool, the Protex server performs DNS lookups for the file comparison server (`sources.blackducksoftware.com`). If the Protex server cannot resolve the DNS lookups, the file comparison tool becomes inoperable.

Statistical Data

This data verifies compliance with the Black Duck agreement. It contains the following information:

- `collectionDate` — Time when data was gathered.
- `collectionPeriod` — Elapsed time since the previous data collection.
- `userCount` — Total number of users.
- `activeUserCount` — Number of users who have logged in since last refresh.
- `userSystemCount` — Total number of unique (user, system) pairs.
- `activeUserSystemCount` — Number of pairs used since last refresh.
- `updateLevel` — Current system update level.

Persistent Resources

This information verifies compliance with the Black Duck agreement. It contains the following:

- `licenseLogins` — Total cumulative logins (authentications, per page).
- `bytesAnalyzed` — Number of bytes processed.

- `filesAnalyzed` — Number of files processed.
- `projectsAnalyzed` — Number of calls to project analysis.
- `bytesCodeprinted` — Number of bytes processed as custom code prints.
- `filesCodeprinted` — Number of files processed as custom code prints.
- `projectsCodeprinted` — Number of projects processed as custom code prints.
- `scanCount` — Number of projects scanned.
- `scanBytes` — Cumulative size of code under management.

Generic System Information

The following generic information is collected for product planning purposes:

- Java runtime environment version.
- Operating system type and version.
- CPU architecture.
- CPUs available to Java.
- Total system memory.
- Maximum memory available to Java.
- Free disk space in the installation directory.
- Free disk space in the database table space directory.

Update Data

- Timestamp
- ID of the update being installed. We do not record whether the installation was successful.

When displaying the file comparison window, if there is no local copy of the reference source (the right-hand pane, showing the source against which the customer code matched), the product requests a copy from `sources.blackducksoftware.com`. Note that this happens only when using the file comparison window, not during project analysis or scans.

When serving reference source requests we log minimal data. This data is stored in the access logs on `sources.blackducksoftware.com`.

- Timestamp
- Reference source file name

Note that we explicitly do not record the requester IP address or any other identifying information.

A

actual licenses

Licenses that are associated with projects in the KnowledgeBase(KB).

ad hoc searches

Searches that look for matches of text entered by a user rather than a saved text search. "Ad hoc" is the Latin term for something done for a particular purpose.

administrator

The individual who handles all system administrative tasks.

aggregated component

A module that functions independently of other modules, and is shipped as part of a collection of modules.

analysis options

System Administrators can globally set the analysis options. If left unchanged, users can set analysis options as they wish.

analyze

Process where Protex compares the contents of source code files to the KnowledgeBase of know licenses and project components.

application server

The main Protex server. Has all components (application server, database, scan/analysis engine)

approval status

The approval process is a way for you to put a final stamp of approval on the accepted projects and licenses. Approval Status can be:* Pending approval Indicated with no visible symbol.* Approved Represented by a green checkmark. * Disapproved Indicated by a red X. During resolution, projects are accepted once they are identified as the origin of code; but there may be any number of reasons why that project should not be used. Using the approval process, you are able to indicate that an additional review was conducted.

approved

An accepted component or license.

archive transversal

Archive files like JAR and ZIP can contain numerous (even thousands of) entries. If kept inside the archive, their respective contents are never matched against the KnowledgeBase (KB). These files could contain third-party files that can create conflicts with your projects. By default, archive files are not set to be opened for analysis. If you want to open them, you have to manually change the Archive Files setting. By opening the archive for analysis all files inside get matched to the KB giving you more accurate results.

Attorney

User role that has priviledges to enter company licenses into Protex; may review and resolve analysis results from analyzed projects; Creates and manages custom licenses. An attorney can also set company policies and resolve issues.

auto identify

Use this feature to perform auto identification on this component. Remember that if applied to a folder, the entire folder is identified - including all files inside.

B

BDS

Black Duck Software

bdstool

A command line interface for Black Duck Export and Protex.

binary matches

The MD5 hash verifies that the two files are identical.

Black Duck updates

KnowledgeBase updates that expand coverage of open source software projects.

BOM

The Bill of Material page lets you examine the properties of any component. It shows you the list of components you have included in your project for shipment.

BSD

Short for Berkeley Software Distribution, the software distribution facility of the Computer Systems Research Group (CSRG) of the University of California at Berkeley. BSD is a family of permissive open source licenses.

C

checksum

A checksum or hash sum is a small-size datum from an arbitrary block of digital data for the purpose of detecting errors which may have been introduced during its transmission or storage. You can configure Protex to use either timestamps or checksums to determine if a file has been changed when rescanning a project.

clone

This is a copy of the original project.

Code Label (TM)

The Code Label tab is a report that displays an easy to read summary of the software contents for a project. The output is similar to food nutrition labels.

code prints

Distinctive digital identifiers for pieces of source code. For example, the digital fingerprint of a custom component.

Compliance Report

Provides an overview of your project status, providing information about whether you are complying with the licenses of your components.

component

A component is a collection of code such as a library, module, or application that is used as a whole unit and is needed when developing or using your software. When you choose your project components, you can select open source components from projects in the KnowledgeBase or you can create custom components.

Component Manager

Feature that allows you to view and modify KnowledgeBase project attributes and obligations. You can also use the Component Manager to create and modify custom components.

component relationship

The relationship of a component to your project, and the resulting license restrictions, conditions, and obligations based on that relationship.

Custom Component Manager

User role with permissions to create projects, add and remove components, resolve issues, review analyis results, and view the KnowledgeBase.

custom fields

You can define a new field to customize your projects. This requires Black Duck Services to provide the initial set-up. Once done, you can fill-in the values for the new field for any project (custom or standard). The new field appears in the project profile page and in Excel reports.

custom licenses

Made-to-order licenses to define attributes and obligations tailored to your particular needs.

custom string search

A custom string search is one that you have created for global use, that is, it is available for all projects.

Customer Support

Call Black Duck Customer Support: 781.891.5100, extension 5

D

declare

This means to include a project or component and set its component relationship. You declare components only on the Bill of Materials tab. You can identify files with no discovered matches. You can also identify a whole directory. You use this to indicate usage of components not included in the analyzed source. You can also use it to define sub-projects in your architecture.

declared

Indicates that the file was manually identified instead of a code match being identified to one of the suggested components.

Detailed Registration Report

This report shows the General Parameters, Mail Settings, Automatic Update Handling Settings, Automatic Installation Schedule, Registration Attributes and Resource Usage Statistics.

Detected File Names

When setting or editing the Detected File Names, it is analogous to setting policy options. Using this feature, you decide which file names to detect. You determine which file names matched require further identification. The list of file patterns represents file types that are often worth reviewing and identifying - even if there are no code matches discovered. You can also use this function to eliminate file names from identification. For example, README files. If your project contains numerous README files you can avoid their detection by removing them from the list of detected file names.

Developer

User role that can perform analysis from the command line and view the KnowledgeBase.

direct code match

This is a match that has been found through analysis, but that has eliminated by a precision or "better" match. This weak match can be shown when using the All filter, and also in the Code Matches All report.

disapproved

A project or license that was refused approval.

distributed

Distributed objects are those you choose package and ship along with your project. When defining whether or not a component is part of an application, if a component is included with the application when it is sold and provided to the end user, it is considered distributed.

Domain Name System (DNS)

It translates domain names to IP addresses. It gives easy names to IP addresses like "Example.org" and not 66.231.100.202.

dual license

A component that has more than one license; usually an open source license and a commercial license.

Dual License Options warning

A warning that indicates that you need to select the other license available for one of the components.

due diligence

A formal review of a company's intellectual property, with a particular focus on open source software (which historically has fallen outside internal controls).

dynamic library

A collection of software functions and/or data that can be used in other programs. Dynamic libraries are linked into a program at runtime. The LGPL definition of a library is a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

E

excluding

Excluding a component indicates that it cannot be matched within a given file or folder. Excluding a component (in-turn) triggers the recomputation of the precision matches in order to find the next best match.

F

File Compararison tool

Feature that lets you drill-down to the file and snippet level to perform a side-by-side comparison of the matched sections of your code and open source code.

file pattern

The type of data that is compared between an application and a code match database. Both text and binary file patterns are compared for maximum effectiveness.

G

GNU

GNU's not UNIX, a UNIX-compatible software system developed by the Free Software Foundation (FSF). The philosophy behind GNU is to produce software that is non-proprietary. Anyone can download, modify and redistribute GNU software. The only restriction is that they cannot limit further redistribution.

GPL

General Public License. The license that accompanies some open source software that details how the software and its accompany source code can be freely copied, distributed and modified. It is assumed that the version is GPLv2 or later if code is not identified otherwise. One of the basic tenets of the GPL is that anyone who acquires the material must make it available to anyone else under the same licensing agreement. The GPL does not cover activities other than the copying, distributing, and modifying of the source code. GPL is also referred to as a "copyleft" in contrast to a copyright that identifies the proprietary rights of material.

H

Help icons

Online Help uses several different types of icons to symbolize the type of help you are viewing. They present a visual representation of the various divisions of help - for concepts, procedures, or reference material.

I

identification

Identification takes place only on the Identify area in the Classic user interface. You use the Identify area to you name the components that are associated with your work. No license knowledge is required. No judgements are made during the identification process. This process is Developers and Managers flagging what code is used in their projects.

identified

The code match was resolved by applying an identification to it.

included code

Code which you intend to copy or modify. You can select code from any open source project in our database, or use your own projects. When the product identifies a code match, there may be several possible sources for the match. If one source is from an Included Project, we assume that is the origin of the code. All other examples of matches to that code are suppressed.

included project

A project from which you intend to copy or modify code. You can select Included projects from any open source project in our database, or use your own projects. When the product identifies a code match, there may be several possible sources for the match. If one source is from an Included Project, we assume that is the origin of the code. All other examples of matches to that code are suppressed.

independent application

Component usage relationshp used for a program that performs a certain broad set of functions. Use this for applications that are very loosely coupled with other applications. Some applications may specify certain areas, such as drivers, as outside the independent application.

integrated application

Component usage relationshp used for applications which have tight relationship with other applications.

Internal Distribution

Usage level that allows internal distribution as defined within a single legal entity or as GPL defines single entity.

IP

Intellectual property.

IP warrant

Certification that the code is free of intellectual property violations.

K

KnowledgeBase

A repository that contains in-depth information about open source and proprietary code licenses and encryption algorithms, including any recent changes, ambiguities, dependencies, incompatibilities, terms, and conditions. Black Duck products draw on this database to automatically review and identify possible issues in code modules and their licenses in the development environment.

L

LGPL

Lesser General Public License. A compromise between the GNU General Public License and simple permissive licenses such as the BSD license and the MIT License. The LGPL places a copyleft restriction on individual source code files but does not copyleft the program as a whole provided you use "a suitable shared library mechanism for linking" and follow certain other restrictions. The LGPL can be linked to software programs that do not have GPL or LGPL.

library

A component that indicates a collection of source files. Often, an aggregation of several modules that are dynamically linked at runtime.

license

A generic contract not associated with a specific product/project that grants a party explicit rights to use intellectual property, for example, a GPL or Apache license.

license attributes

License requirements encoded into a machine readable format. Protex compares license attributes to determine compatibility and conflicts.

license conflict warning

A warning that indicates a possible incompatibility between the licenses of two or more components in the project hierarchy.

License Manager

Feature that enables attorneys to create customized licenses for use in analysis of license conflicts and in the implementation of business policies, and provides other features specifically developed to facilitate the involvement of in-house or outside counsel in the timely review of issues arising in the development process.

Limited External Distribution

Usage level that allows distribution to unrelated, external entities, but not for further redistribution.

local string search

A local string search is one that you have created for a specific project. It is not available for use by other projects.

M

machine code

The native language of the computer. In order for a program to run, it must be presented to the computer as binary-coded machine instructions. Machine language is created by programs called "assemblers," "compilers" and "interpreters," which convert the lines of programming code a human writes into the machine language the computer understands.

managed code base

This is a code base owned or controlled by the end user that is input into a product by an end user and managed using that product over the course of the applicable subscription period. The size of the managed code base equals the aggregate of code added to the managed code base, whether or not any of that code is eventually deleted by end user.

Manager

User role that has the ability to create projects from the web application and assign members to projects.

MB Estimation Tool

The MB Estimation Tool allows you to make an estimate of how much code is in your project, before you start the analysis process. You may want to divide a large project into smaller subprojects to reduce analysis time. Some Black Duck licenses are based on the size of the projects you are going to scan. The MB Estimation Tool lets you make an estimate of how many megabytes of capacity you will need to purchase to analyze your code.

module

Collection of source files that generally is not shipped alone. Separate modules of software are usually distributed in conjunction with a program under their own license agreement and are not derivative works of the program. IBM Public License distinguishes between Contributions that constitute changes or additions to the program which are deemed to be "contributions", and "additions to the program which (i) are separate modules of software distributed in conjunction with the Program under their own license agreement and (ii) are not derivative works of the program."

N

non-distributed

Non-distributed objects are those needed for your project code that you do not distribute. Sometimes, you may require end users to supply these projects on their own.

O

obligations

Requirements that must be fulfilled to comply with the license. They are not analyzed for conflicts, but are additive.

Open Source

Code that is available to the general public for use and/or modification from its original design free of charge. Examples of popular open source programs are the Apache Web server and the Linux operating system. Using open source code may obligate developers to include certain information or control distribution in ways specified in the license.

Options

Resolution: 1. I am ok with this project. If this project is found as the only code match of a file, then this project is the origin of the code and the file is resolved. This project will be part of the license computation as long as a code match is found. 2. I know I have code from this project. If this project is found as the only match of a file, then this project is the origin of the code and the file is resolved. This project will be part of the license computation. 3. I am ok with this project. If this project is found among the exact code matches of a file, then this project is the origin of the code and the file is resolved. This project will be part of the license computation as long as a code match is found. 4. I know I have code from this project. If this project is found among the code matches of a file, then this project is the origin of the code. Include the project in the license computation even if code matches are resolved to other projects.

OSS

Open Source Software.

P

pending approval

Waiting to be approved or rejected.

personal use

Usage level that allows any use of code for personal purposes only.

PostgreSQL

PostgreSQL is a free object-relational database server (database management system), released under a flexible BSD-style license.

Power Developer

User role with the permission to create projects, add and remove components review analysis results, run analysis, and view the KnowledgeBase.

Precision Matching (TM)

Precision Matching is a technique to reduce the number of possible code matches when dealing with large numbers of code matches.

Prerequisite

A prerequisite is something the project requires, but that is being released as part of the project. For example, a library that is not shipped with the project but required for its operation.

project

These are the sources used in your own project or product (not open source in origin).

project component

A project, product, or piece of code that is required to develop or use your project.

Project Leader

User role with permissions to run analysis, review analysis, resolve issues, and create new projects.

project license

A project license is the license used for the distribution of your project. When you analyze your code, Protex reports any license violations and obligations based on the project license.

proprietary

Privately owned and controlled by one company that has not divulged specifications that would allow other companies to duplicate the product. This is the opposite of open source.

R

rejected

A code match was found and reported in the system, but the user rejected it. This causes Precision matching to re-calculate and the next best match is suggested in return.

roles

Protex uses roles to determine the tasks a user can perform. These correspond to typical job titles/functions such as Administrator, Attorney, Developer, or Manager.

S

Sarbanes-Oxley

An act of the United States Congress that requires a company to report the value and use of intellectual property assets as they affect the financial condition of the company and enable investors to assess the company as a whole.

search

The automatic matching of text strings in the source code files with the text strings in the KnowledgeBase. Search occurs during code analysis.

snippet

This is a small re-usable piece of computer code.

source code

Program instructions in their original form, which is the only format readable by humans. Initially, a programmer writes a program in a particular programming language. To execute the program, however, the programmer must translate it into machine code, which is the language that the computer understands.

SSL

Secure socket layer. A cryptographic protocol that provides secure communications on the Internet.

static library

A collection of software functions and/or data that can be used in other programs. Static libraries are linked into a program at link time. The LGPL definition of a library is a "collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables."

string match

The occurrence of a string of alphanumeric characters in a source code file that is identical to any text string stored in the KnowledgeBase.

system logs

You can view a variety of logs from the GUI. Use the Search feature to select a specific log or to point to a specific directory path of logs. You can also use the Show filter to view a specific type of log file.

T

template licenses

Used when an actual license is not known, or as a basis to create a custom license.

U

usage levels

Usage levels are the point at which license restrictions and conditions take effect based on how you intend to use and distribute the code. Selecting a usage identifies how the component (or other item) is connected to the project.

V

versions

Versions in the Black Duck KB let you Identify specific versions of components used in your code. The specific version being used could become particularly important as projects change licenses between versions.

Index