BLACKDUCK | Protex

Installation Guide

7.8.9

This edition of the *Installation Guide* refers to version 7.8.9 of Protex.

This document created or updated on Wednesday, February 7, 2024.

Please send your comments and suggestions to:

Synopsys
800 District Avenue
Suite 201
Burlington, MA 01803-5061 USA

Copyright © 2024 by **Synopsys, Inc.**

All rights reserved. All use of this documentation is subject to the license agreement between Black Duck Software, Inc. and the licensee. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the prior written permission of Black Duck Software, Inc.

Black Duck, Know Your Code, and the Black Duck logo are registered trademarks of Black Duck Software, Inc. in the United States and other jurisdictions. Black Duck Code Center, Black Duck Code Sight, Black Duck Hub, Black Duck Protex, and Black Duck Suite are trademarks of Black Duck Software, Inc. All other trademarks or registered trademarks are the sole property of their respective owners.

Contents

Chapter 1: Protex Product Overview **8**
1.1 Protex Architecture Overview 8
1.1.1 Protex Servers 9
1.1.2 Protex Databases 10
1.1.3 Scan Repository 10
1.1.4 Protex Browser Requirements 11
1.1.5 Protex Client 11
1.1.6 Protex Connectivity Requirements 12
1.2 Before You Begin – Checklist 12
Chapter 2: Server Installation **14**
2.1 Recommended Hardware Requirements - Protex Server 14
2.1.1 Protex and Virtual Machine (VM) Restrictions 15
2.2 Operating System Requirements - Protex Server 17
2.3 Step 1 - Mounting the Drive 17
2.3.1 Automatically Mounted Drive 18
2.3.2 Manually Mounting the Drive (Mounted with noexec flag) 18
2.3.3 Manually Mounting the Drive - SUSE 19
2.3.4 Manually Mounting the Drive - Red Hat 20
2.4 Step 2 - The Installation Process 21
2.4.1 Installing Protex as a Non-root User 21
2.4.2 Installing the Protex Server 22
2.4.3 Installing the Protex Server Using Console Mode 31
2.5 Step 3 - Unmounting the Drive 36
2.6 Installing from ISO Images 36
2.7 Server Registration 36
2.7.1 Before You Begin - Registration 36
2.7.2 Registering the Server 37
2.7.3 Testing Your Server Installation 38
2.7.4 Detailed Product Registration Report 39
Chapter 3: Client Installation Overview **41**
3.1 Recommended Hardware Requirements - Protex Client 41
3.2 Operating System Requirements - Protex Client 41
3.3 Before You Begin - Client Installation 42

3.4 Installing the Client 42
3.5 Client Installation on Linux 42
3.6 Client Installation on Mac 49
3.7 Client Installation on Windows 51
3.8 Configuring Server Access to Source Code 57
3.9 Configuring Default Client Settings 58
3.10 Configuring the Client for SSL 58
Chapter 4: Upgrading Protex 61
4.1 Updating the Black Duck KnowledgeBase 61
4.2 Upgrading the Protex Server 61
4.3 Upgrading the Protex Client 62
4.4 Debugging and Troubleshooting 63
4.5 Recovering a Protex Server 64
Chapter 5: Uninstalling Protex 65
5.1 Un-installing the Protex Server 65
5.2 Uninstalling the Client Application 67
Chapter 6: Managing your PostgreSQL database 70
6.1 PostgreSQL Replication Slots 70
6.2 Database Settings with PostgreSQL 70
6.3 Database Backup with PostgreSQL 70
Appendix A: Protex Log Files 71
A.1 Viewing Log Files 71
A.2 Log Files 73
Appendix B: Calculating Upgrade Requirements 75

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.
Hardware Software Specifications	PDF_HW_SW_Spec.pdf	Protex and Code Center hardware/software specifications, requirements, and recommendations.

Customer Support

For the latest in web-based support, access the Synopsys Customer Support web site: https://community.synopsys.com/s/welcome-to-the-synopsys-community.

To access a range of informational resources, services and support, as well as access to Synopsys experts, visit the Synopsys Customer Success portal at: https://community.synopsys.com/s/welcome-to-the-synopsys-community.

You can also contact Synopsys Support by:

- **Email**: community.manager@synopsys.com
- **Phone**: To reach us by phone, refer to the Contact Us section at the bottom of our support page to find your local phone number.
- **Fax**: +1 781.891.5145

Standard office hours are Monday through Friday 8:00 AM to 8:00 PM US EST.

Note: Customers on the Enhanced Customer Support Plan are able to contact customer support 24 hours a day, 7 days a week to obtain Tier 1 support.

Training

Black Duck Synopsys training courses are available for purchase. Learn more at https://community.synopsys.com/s/education.

View the full catalog of our online offerings: https://community.synopsys.com/s/education.

When you are ready to learn, you can log in or sign up for an account: Synopsys Software Academy.

Services

If you would like someone to perform Protex tasks for you, please contact the Synopsys Professional 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 Synopsys products.

Contact Synopsys Professional Services at https://www.synopsys.com/cgi-bin/sps/contact/contact.cgi, or engage your Synopsys account team for more information.

Synopsys Software Integrity Group (SIG) Community

The Synopsys Software Integrity Group (SIG) Community is our primary online resource for customer support, solutions, and information. The community allows users to quickly and easily open support cases and monitor progress, learn important product information, search a knowledge base, and gain insights from other SIG customers. The many features included in the community center around the following collaborative actions.

- Connect – Open support cases and monitor their progress, as well as monitor issues that require engineering or product management assistance.
- Learn – Insights and best practices from other SIG product users to allow you to learn valuable lessons

from a diverse group of industry leading companies. In addition, the community puts all the latest product news and updates from Synopsys at your fingertips, helping you to better utilize our products and services to maximize the value of open source within your organization.

- Solve – Quickly and easily get the answers you're seeking with the access to rich content and product knowledge from SIG experts and our KnowledgeBase.
- Share – Collaborate and connect with SIG staff and other customers to crowd source solutions and share your thoughts on product direction.

Access the community: If you do not have an account or have trouble accessing the system, click here to get started, or send an email to community.manager@synopsys.com.

To see all the ways you can interact with the Synopsys Software Integrity Group Support, visit: https://www.synopsys.com/software-integrity/support.html.

Chapter 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.

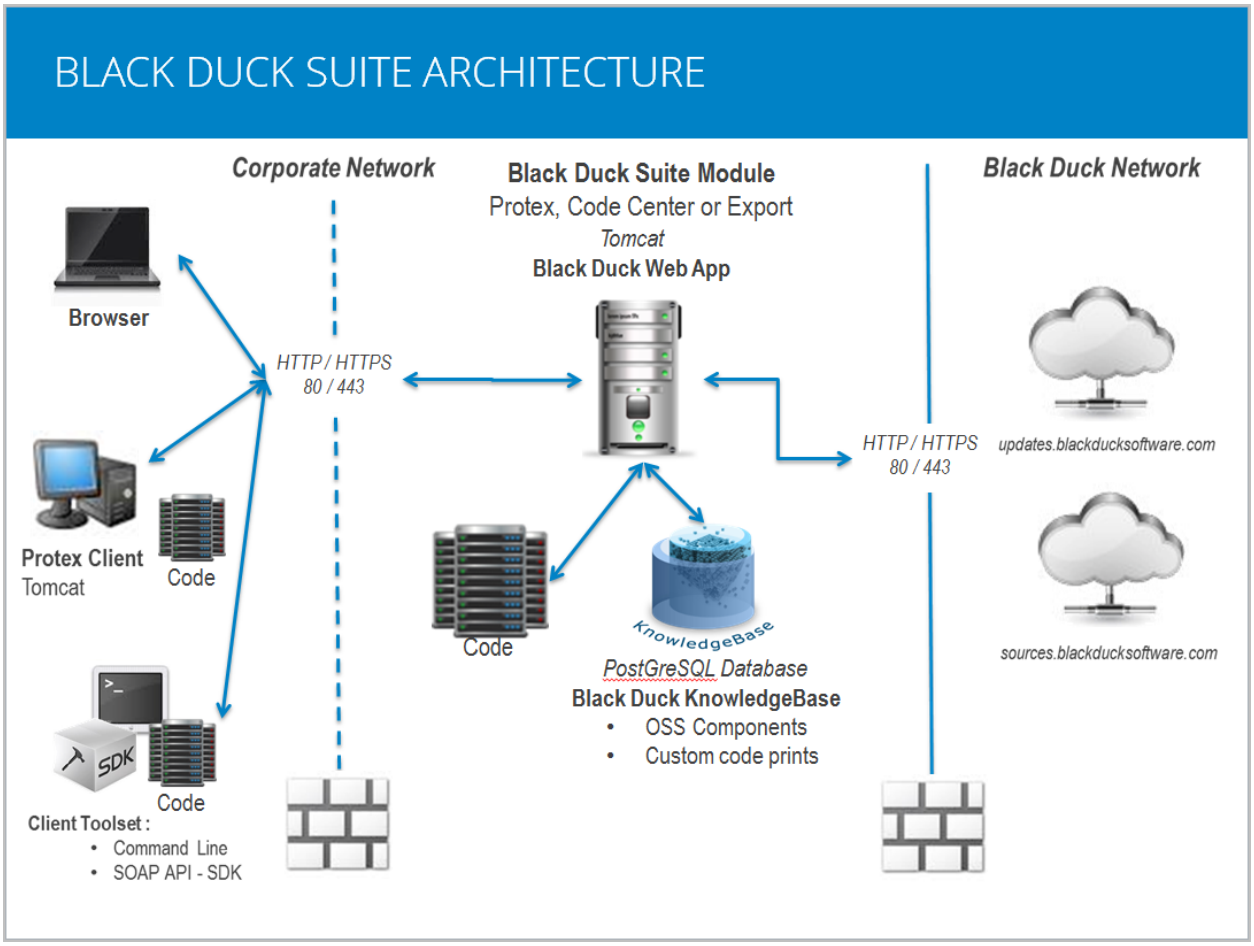
Protex manages the complexity of license obligations by providing accurate, up-to-date component and licensing information to legal counsel, developers, and managers. By enabling the proactive management of component software, Protex reduces personnel and development costs, improves time-to-solution,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

1.1 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



1.1.1 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.

1.1.2 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.

1.1.3 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.

1.1.4 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.

1.1.5 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.

1.1.6 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 servers.

Note: To properly communicate with the following servers, you must whitelist the entire Black Duck IP address range of 192.231.134.0/24 (192.231.134.1-254).

Table 1.2: Connectivity Requirements

URL	Description
updates.protex.blackducksoftware.com	Black Duck Update server – Provides periodic Protex software and KnowledgeBase updates to customers.
sources.blackducksoftware.com updates.blackducksoftware.com	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.
updates.codecenter.blackducksoftware.com	Black Duck Update server – Provides periodic Code Center software updates to customers.
updates.codesight.blackducksoftware.com	Black Duck Update server – Provides periodic CodeSight software updates to customers.
updates.suite.blackducksoftware.com	Black Duck Update server – Provides periodic Suite software updates to customers.
dl.blackducksoftware.com	Black Duck server – Provides Code Center deep license data.
kb.blackducksoftware.com	Black Duck server – Provides access to the Hub KnowledgeBase in the cloud (port 443 only).

- Connectivity to the application server and Internet from the internal clients through a static proxy is also acceptable.

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

1.2 Before You Begin – Checklist

Before you begin the installation, verify the following:

- **Registration Key** – In order to use the system, you need a registration key and are required to register via the web after installation. This registration key accompanies your installation kit. If you do not have a registration key please contact Black Duck Customer Support. See the Preface on page 5 for contact information.

Note: Application server registration keys are different from scan server registration keys. Protex requires a registration key for the application server and each additional scan server requires a separate registration key.

- **Memory Settings** – Make sure you record all memory settings for processes that you may have re-configured. The installation process overwrites the modified settings. These settings must be manually reset after the installation. You may want to contact Customer Support for help.
- (Optional) **PKCS12 keystore** - During the installation, you are asked if you want to use an HTTPS connection to access the Protex server. If you plan to use HTTPS, you should import your keystore data before you run the installer. Protex uses the PKCS12 keystore format. For specific information about configuring Protex for SSL, refer to the Protex *System Administrator Guide.*

Note: Server installations or upgrades can take several hours, depending upon the database sizes. Please plan accordingly.
The installation program (InstallAnywhere) makes use of the `/tmp` directory for temporary files. If you have insufficient space on this device, you can set an environment variable used by the installer to point to another device: `export IATEMPDIR=<new-directory-name>`.
Space requirements vary, but plan at least 5 - 10 GB of free space during an upgrade.

Chapter 2: Server Installation

This chapter provides the details on installing the Protex server software. It gives in-depth details for the various possibilities to make your installation operation easier. Simply choose the correct procedure for your specific situation.

You can install the Black Duck Protex server by using: a graphical user interface (GUI) installation, console mode, or by using silent mode.

This chapter details a new installation. The Protex installation consists of three phases, as follows:

1. Mounting the drive.
2. Installing the software.
3. Unmounting the drive.

The sections that follow provide the details for each phase of the installation.

Tip: Code Center, Protex, and [[[Undefined variable Variables.Short Company Name]]] Hub must be installed on dedicated and separate servers.

2.1 Recommended Hardware Requirements - Protex Server

To set up the Protex server for best results, configure your storage devices to effectively process high amounts of disk I/O in support of the large database that comes with the product. This section describes the hardware requirements and different approaches for configuring your hard drives for optimal performance.

When checking your hardware for the installation of Protex, we recommend that you purchase a machine with the capability to handle two separate storage arrays, installed on an advanced RAID controller. Maintain enough free space to allow Protex room to create scratch tables during scanning. The size required is dependent on the number of matches produced by a scan, whether the scan is full or incremental, and the number of concurrently running scans.

The following sections describe the recommended minimum hardware for several deployment scenarios. The installation process checks for a minimum of 1 TB of free space, although more free space is strongly recommended.

Note: Black Duck does not recommend specific brands of processors; only the minimum capabilities available in the suggested options.

Tip: For optimal database performance, we recommend RAID 10 for the database partition.

For additional hardware information, refer to Recommended Project Sizes and Project Size Limitations.

Minimum departmental server requirements (10 to 20 users)

- Processor: Two Core 2 Quad 64-bit processors (Intel® Xeon® or AMD Ryzen)
- RAM: 32 GB
- Storage: Local attached storage (preferred) or SAN disk storage (fiber channel)
- Drives: 10K – 15K RPM SCSI/SAS drives required
- RAID: Controller capable of managing multiple RAID arrays:
    - Array 1 = Two 146 GB disks mirrored (RAID 1) (configured as "/" for OS and Protex). This space is used for online updates and your project source code.
    - Array 2 = 14 dedicated 15K RPM 300 GB disks or eight dedicated 10K RPM 500 GB disks in RAID 10 configuration (configured as `/var/lib/bds-protexip` for the database).

Note: Add sufficient disk space to yield approximately 3 TB of usable storage after formatting for the database partition.

Enterprise server requirements (20 to 40 users)

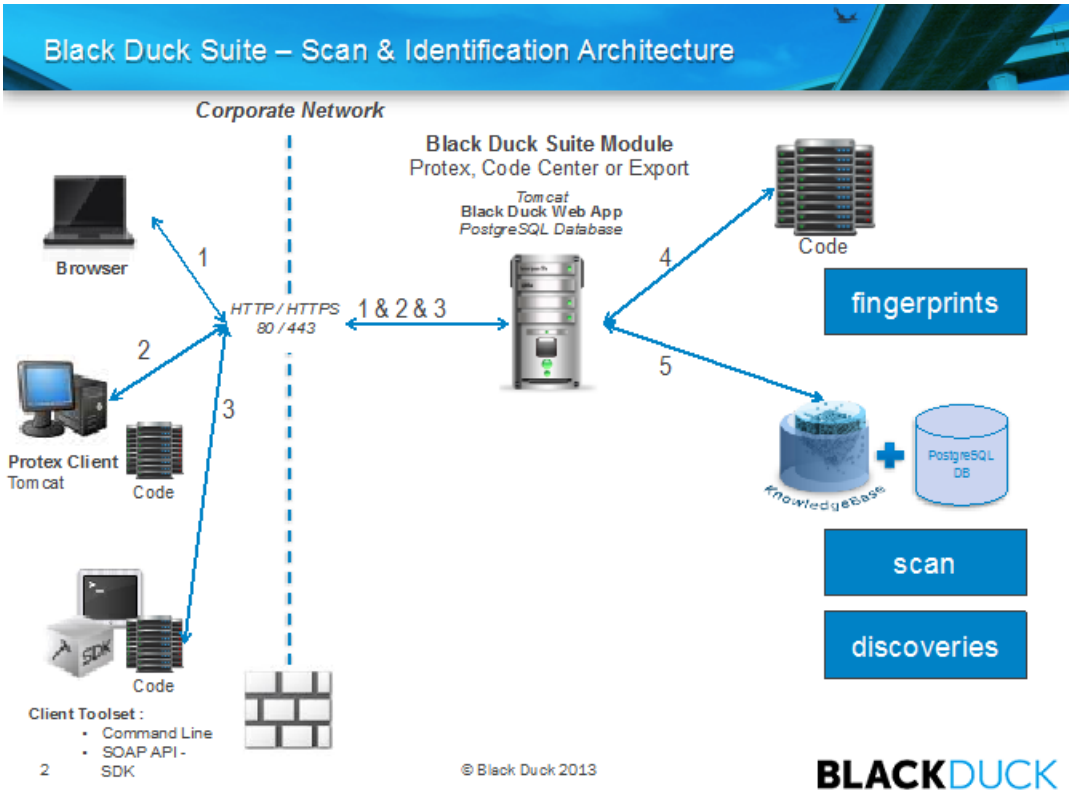
- Processor: Two eight-core 64-bit processors (Intel® Xeon® or AMD Ryzen)
- RAM: 64 GB
- Storage: Local attached storage (preferred) or SAN disk storage (fiber channel)
- Drives: 15K RPM SCSI/SAS drives required
- RAID: Controller capable of managing multiple RAID arrays:
    - Array 1 = Two 146 GB disks mirrored (RAID 1) (configured as "/" for OS and Protex). This space is used for online updates and your project source code.
    - Array 2 = Add sufficient disk space to yield approximately 4 TB of usable disk storage in a RAID 10 configuration after formatting (configured as `/var/lib/bds-protexip`) for the database.

Tip: We recommend that you contact Black Duck Services to help set up larger configurations.

2.1.1 Protex and Virtual Machine (VM) Restrictions

Protex has high I/O activity during scanning, identification, and report creation. The following diagram illustrates the read/write connection points.

Figure 2.1: Read/write Operations



Due to the high I/O requirements, Black Duck does not recommend that Protex be installed and run in a virtual machine (VM). Protex performance is slowed by the abstraction layer between the VM and the disk that adds overhead for all I/O operations. Monitoring of Protex in VMs has shown high levels of CPU inefficiencies due to high I/O wait states. This behavior is expected in virtual environments or in non-virtual environments with storage not optimized for high I/O activities.

While running scans, Protex collects data from the files being scanned to create the signatures needed for matching. The read activity happens where the code is located: on the local client for client-side scans (2 and 3), and on the server for server-side scans (4). In the case of client-side scans, this data is sent over the network to the Protex server.

Protex writes the scanned file data into the database (5), and also stores certain data on the file system (4), including log files and temporary files. Protex then analyzes the data by reading the scan data from the database (5), processing and comparing results against the KnowledgeBase (5) and the fingerprints stored on the application server file system (4) to provide results presented in the Protex user interface. The results data is also written to the database (5). The process of collecting scan data, writing to the database, analyzing to provide results is done incrementally during the scan and analysis with many read/write activities between the application and the database, as well as some file system read/write activities. Client-side scans require constant connection to the Protex application server since data is typically uploaded 1 - 3 files at a time (2 & 3).

As the user works in their browser (1) to view and act on the results of the Protex analysis, data is read from the database (5) and sent to the user's browser. In cases where the scanned project contains a lot of open source code, the quantity of data read from the database and sent to the browser can be large. When users

create reports, very large data sets are read from the Protex application server and sent back to the user's system.

If Protex must be run on a VM, Black Duck recommends the following configuration parameters for the best possible performance:

- Provide the fastest physical storage possible.
- We do not recommend using virtual disk images.
- Provide the fastest possible I/O. We recommend 10GbE or FC for network mounted drives.
- Take into account the I/O requirements of Protex partitions, listed in order of increasing requirements:
  - `/var/lib/bds-protexip` (PostgreSQL database and finger prints)
  - `/opt/blackduck/protexIP`
  - `/home/blackduck`
- Follow the standard recommendations for RAIDs.
- Consider that performance is directly affected by the size of the server and the number of VMs running on the server.
  - Logical cores dedicated to the VMs should not exceed the physical cores on the host.
  - Virtual memory dedicated to the VMs should not exceed the physical memory on the host.

2.2 Operating System Requirements - Protex Server

Our goal is to test Black Duck products with the latest revision of the two most recent operating system releases. We encourage you to update to the latest minor version of your operating system as new versions are released.

In general, we support the major operating system releases and all subsequent minor releases. New operating system updates are continually being released. If you do not see a minor release listed, we recommend testing compatibility before implementing in a production environment.

For a complete listing of the platforms that are tested and supported for this release, refer to the Supported Operating Systems topic in the *Black Duck Hardware Software Specifications*.

2.3 Step 1 - Mounting the Drive

This installation requires the use of a USB drive. Typically USB drives are mounted into the following path: `/media`. In the examples that follow, this is the directory used.

Since there are several variations of operating systems, it is impractical to provide examples for all possibilities. However, the examples used in this installation manual represent the most common scenarios. Your particular situation may vary somewhat. If using Red Hat, the media is mounted under: `/media/usbdisk`.

There are three possible circumstances as follows:

- The USB drive is automatically mounted – The drive is automatically mounted to `/media/PROTEXIP`. In Red Hat, it is mounted under: `/media/usbdisk`.

- The USB drive mounted with the `noexec` flag set – The drive is mounted but needs to be remounted.
- The USB drive is not automatically mounted – You must manually mount the drive and start the installation.

Select the situation for mounting your installation drive from the following three circumstances:

2.3.1 Automatically Mounted Drive

To verify that the drive is mounted to the proper location:

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

```
protexIP-:~ # mount
```

Here is a typical display for SLES 10:

```
/dev/sdb2 on / type ext3 (rw,acl,user_xattr)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
debugfs on /sys/kernel/debug type debugfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
securityfs on /sys/kernel/security type securityfs (rw)
/dev/sdc1 on /media/PROTEXIP type vfat
(ro,nosuid,nodev,flush,shortname=winnt,utf8,uid=0)
```

On a Windows system, the device should mount automatically when you plug it into a USB port. The device is listed as a new volume in the display.

Proceed to Step 2 - The Installation Process on page 21 to begin the installation.

2.3.2 Manually Mounting the Drive (Mounted with noexec flag)

To mount the drive to the proper location:

Note: This example assumes that the external disk drive is mounted under `/media/PROTEXIP`.

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

```
protexIP-:~ # mount
```

Here is a typical display:

```
/dev/sdb2 on / type ext3 (rw,acl,user_xattr)
proc on /proc type proc (rw)
```

```
sysfs on /sys type sysfs (rw)
debugfs on /sys/kernel/debug type debugfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
securityfs on /sys/kernel/security type securityfs (rw)
/dev/sdc1 on /media/PROTEXIP type vfat
(rw,noexec,nosuid,nodev,flush,shortname=winnt,utf8,uid=0)
```

3. Issue the following command to remount the drive:

```
protexIP-:~ # mount -o remount,ro,exec /media/PROTEXIP
```

4. Check to see if it is properly mounted as described in Automatically Mounted Drive on page 18.
5. This ends Phase 1 of the installation process. Proceed to Step 2 - The Installation Process on page 21 to begin the installation.

2.3.3 Manually Mounting the Drive - SUSE

To mount the drive to the proper location:

Note: This example assumes that the external disk drive is mounted under `/media/PROTEXIP`.

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

```
protexIP-:~ # mount
```

Here is a typical display:

```
/dev/sdb2 on / type ext3 (rw,acl,user_xattr)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
debugfs on /sys/kernel/debug type debugfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
securityfs on /sys/kernel/security type securityfs (rw)
```

3. Enter the following command to identify the device:

```
dmesg | grep -A 15 "usb-storage: device found"
```

Here is a typical display:

```
usb-storage: device found at 5
usb-storage: waiting for device to settle before scanning
    Vendor: Seagate   Model: FreeAgent Go      Rev: 100F
    Type: Direct-Access       ANSI SCSI revision: 04
```

```
SCSI device sdc: 156301488 512-byte hdwr sectors (80026 MB)
sdc: Write Protect is off
sdc: Mode Sense: 1c 00 00 00
sdc: assuming drive cache: write through
SCSI device sdc: 156301488 512-byte hdwr sectors (80026 MB)
sdc: Write Protect is off
sdc: Mode Sense: 1c 00 00 00
sdc: assuming drive cache: write through
 sdc: sdc1
sd 7:0:0:0: Attached scsi disk sdc
sd 7:0:0:0: Attached scsi generic sg2 type 0
usb-storage: device scan complete
```

In this example, the device is **/dev/sdc1**.

4. Mount the drive by entering the following commands:

```
mkdir /media/PROTEXIP
mount -t vfat -o ro /dev/sdc1 /media/PROTEXIP
```

Proceed to section Step 2 - The Installation Process on page 21 to begin the installation.

2.3.4 Manually Mounting the Drive - Red Hat

To remount the drive to the proper location:

Note: This example assumes that the external disk drive is mounted under `/media/PROTEXIP`.

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

```
dmesg | grep -A 15 "Seagate"
```

Here is a typical display for Red Hat:

```
usb 1-3: new high speed USB device using address 7
scsi7 : SCSI emulation for USB Mass Storage devices
   Vendor: Seagate   Model: Portable      Rev: 0130
   Type: Direct-Access      ANSI SCSI revision: 02
SCSI device sdc: 488397168 512-byte hdwr sectors (250059 MB)
sdc: assuming drive cache: write through
SCSI device sdc: 488397168 512-byte hdwr sectors (250059 MB)
sdc: assuming drive cache: write through
```

```
sdc: sdc1
Attached scsi disk sdc at scsi7, channel 0, id 0, lun 0
USB Mass Storage device found at 7
```

In this example, the device is `/dev/sdc1`.

3. Mount the drive by entering the following commands:

```
mkdir /media/PROTEXIP
mount -t vfat -o ro /dev/sdc1 /media/PROTEXIP
```

Proceed to section Step 2 - The Installation Process on page 21 to begin the installation.

2.4 Step 2 - The Installation Process

This section describes several ways to install the software. The installation can be performed in three modes, as follows:

- Console Mode – (Linux only) Runs from the command line and requires user interaction.
- GUI – Runs in interactive mode with a graphical user interface.
- Silent Mode – (Linux only) Runs from the command line and accepts all system defaults. Does not require user interaction.

Select the proper method for your circumstances.

Note: When upgrading Protex on Windows, you must update your Protex instance by running the ISO file.

2.4.1 Installing Protex as a Non-root User

You can install Protex server and client even if you are not a root user. You can accept the installation default values, or create your own customized installation. Both options are described as follows.

To install Protex as a non-root user with the default installation values:

1. In the ISO installation media, login as *root*.
2. Run the command `./ProtexPreInstallNonRootUserSetup.sh`. Use this option if you are accepting all the default installation values, which are:
   - `PROTEX_USER` = bds-protexip
   - `PROTEX_GROUP` = bds-protexip
   - `PROTEX_INSTALL_DIR = /opt/blackduck/protexIP`
   - `PROTEX_HOME_DIR = /var/lib/bds-protexipor`
3. When prompted, specify a password for *bds-proextip*.
4. Log in as *bds-protexip* to run the installation.

To install Protex as a non-root user with customized installation values:

1. In the ISO installation media, login as *root*.
2. Run the command `./ProtexPreInstallNonRootUserSetup.sh Protex_User Protex_Group /opt/Protex/ /var/lib/Protex/` . All your custom values must be entered as a single command. The command shown in this step is just an example; after `./ProtexPreInstallNonRootUserSetup.sh`, you must specify values, separated by a space, for:
    - Protex_user
    - Protex_group
    - Protex_installation_directory
    - Protex_home_directory
3. The following information displays so you can review it. The installation directory must end with `protexIP` and is appended if necessary. User's home directory must end with your user login name; it is also appended if necessary.
    a. Setup Summary:
    b. User Name: `Protex_User`
    c. Group Name: `Protex_Group`
    d. Installation Directory: `/opt/Protex/protexIP`
    e. User's Home Directory: `/var/lib/Protex/Protex_User`
4. When you are satisfied that the preceding information is correct, press **Enter** to continue.
5. To use a domain user which does not exist in `/etc/passwd`, manually add the user to `/etc/passwd` before running `./ProtexPreInstallNonRootUserSetup.sh`, and then remove it after the command has run.
6. Setting up your home directory occurs at the end of the script. If it failed, you may see the following message, which can be ignored if you are the domain user.
   Setting /var/lib/Protex/Protex_User as the Protex_User user's home directory. Failed to set Protex_User's home directory. Please make sure that Protex_User is logged out completely from the system. Run /tmp/ProtexPreInstallNonRootUserSetup.sh again.
7. When prompted, specify a password for the user.
8. Log in with the username you specified to run the installation.

2.4.2 Installing the Protex Server

You must have *root* (Linux) or *admin* (Windows) privileges to install the Protex server.

To install the Protex server:

Note: This example assumes that the external USB drive is mounted under `/media/PROTEXIP` on Linux or `D:` on Windows.

1. Enter the following command to change directories:

```
cd /media
```

Or

```
cd D:
```

2. Run the installation script to start the GUI installer:

```
./PROTEXIP/install.sh (on Linux)
```

Or

```
D:\install.bat (on Windows)
```

On Linux, you have also the option of installing using console mode.

```
./PROTEXIP/install.sh -i console
```

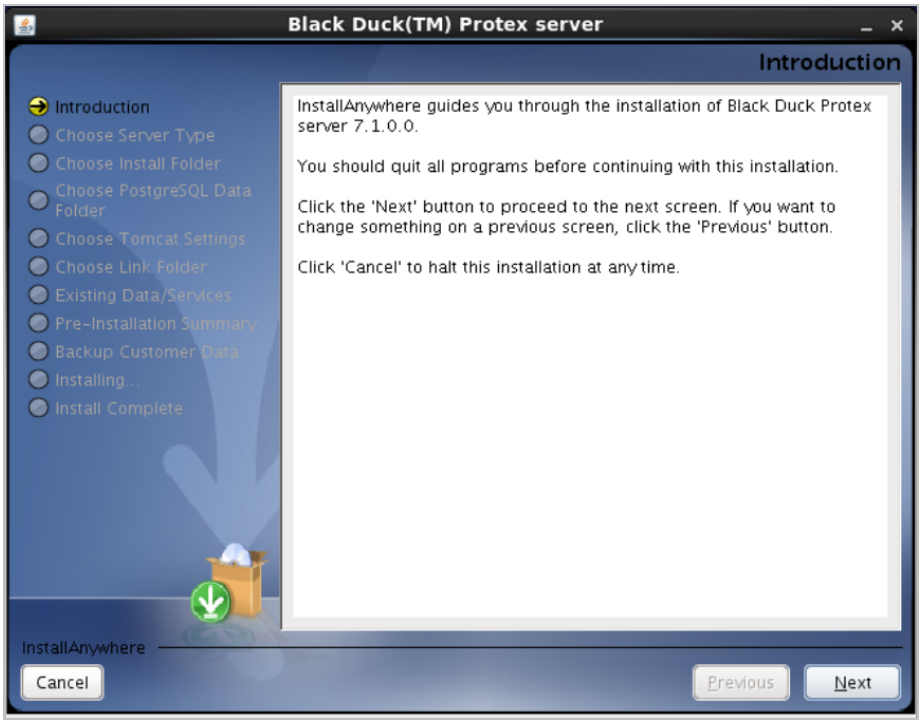
Or

```
./PROTEXIP/install.sh -i silent
```

Note: Refer to Installing the Protex Server Using Console Mode on page 31 for more information on using console mode.

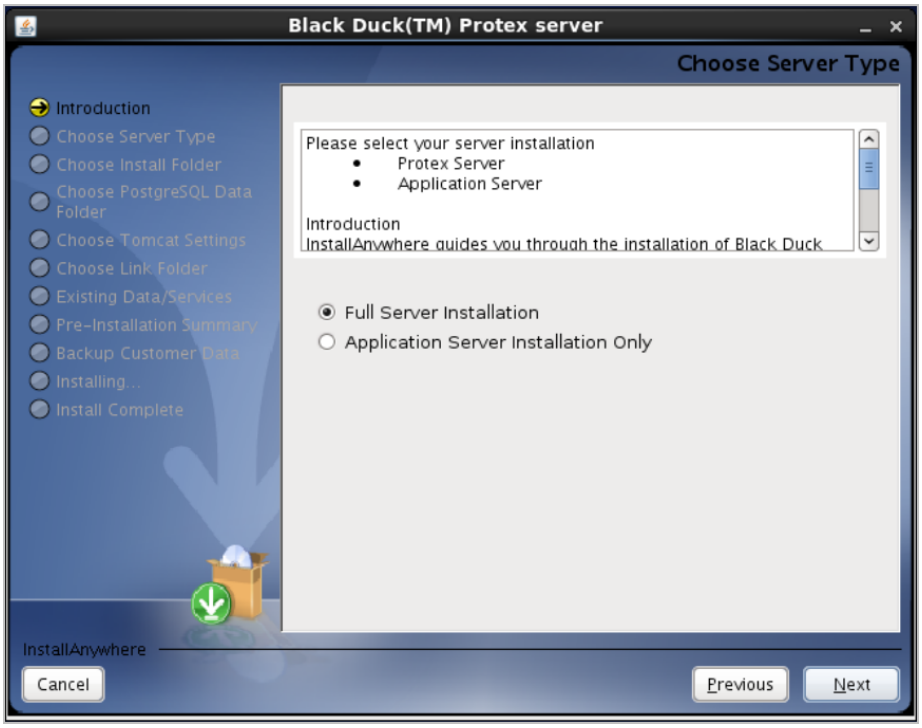
The installer launches. These screen captures are from a Linux system, but the Windows install is similar:

Figure 2.2: Server - Introduction



3. Click **Next**.

Figure 2.3: Server - Choose Server Type

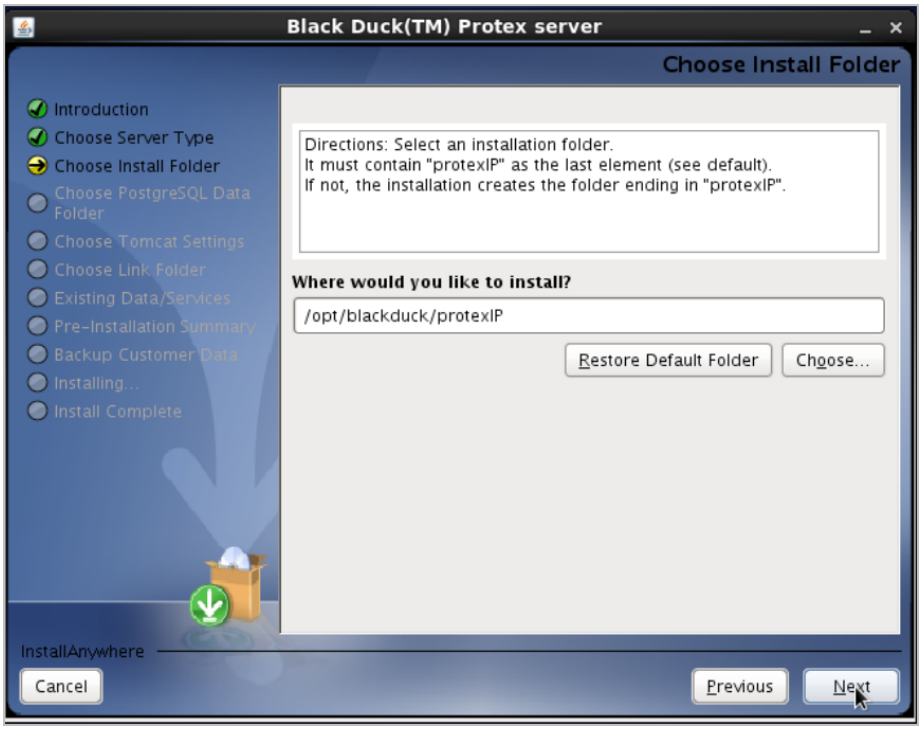


4. In the **Choose Server Type** screen, select the option that matches your implementation. Note that two separate installs are required to install both the application server and the scan server. For more information, refer to the section *Implementing Multi-server Environments* in the Protex *System Administrator Guide*.

If you are installing	Select
Single server Protex implementation	Full Server Installation
Multi-server synchronization implementation - Primary server	Full Server Installation
Multi-server synchronization implementation - Secondary server	Full Server Installation
Multi-server scan implementation - Application server	Application server installation only. (Only the Application Server is installed with the feature to add scans servers enabled by default.)
Multi-server scan implementation - Scan server	Has a separate installer. Cancel and launch `install_scan.sh` instead.

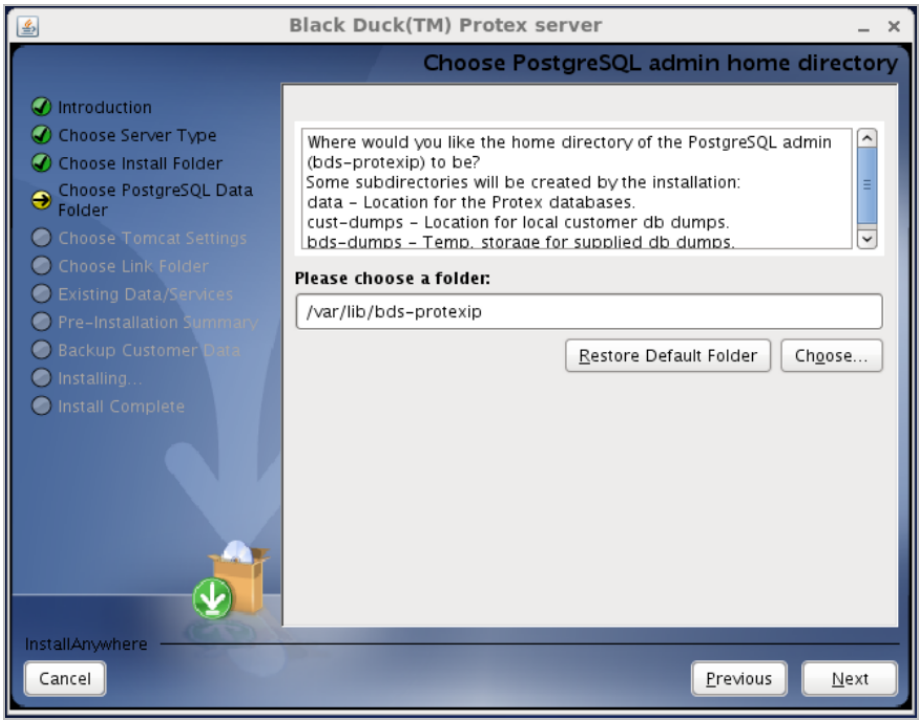
5. Click **Next**.

Figure 2.4: Server - Choose Install Folder



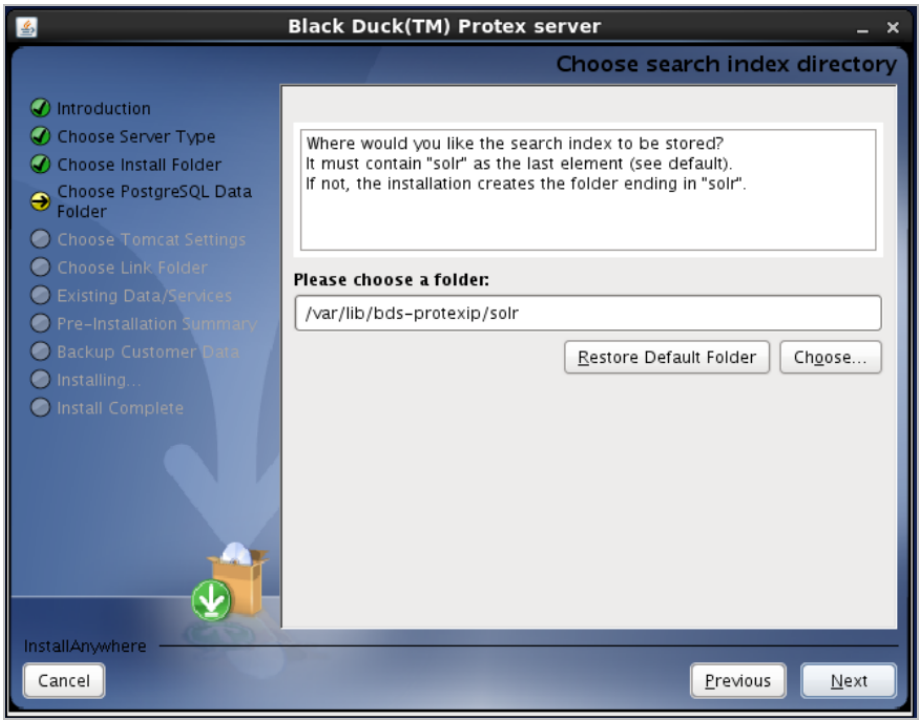
6. On the **Choose Install Folder** screen, specify a directory for the installation. The default directory is `/opt/blackduck/protexIP`. Click **Choose** to browse for a particular directory. Click **Restore Default Folder** to re-establish the original default setting.

Figure 2.5: Server - Choose PostgreSQL Admin Home Directory



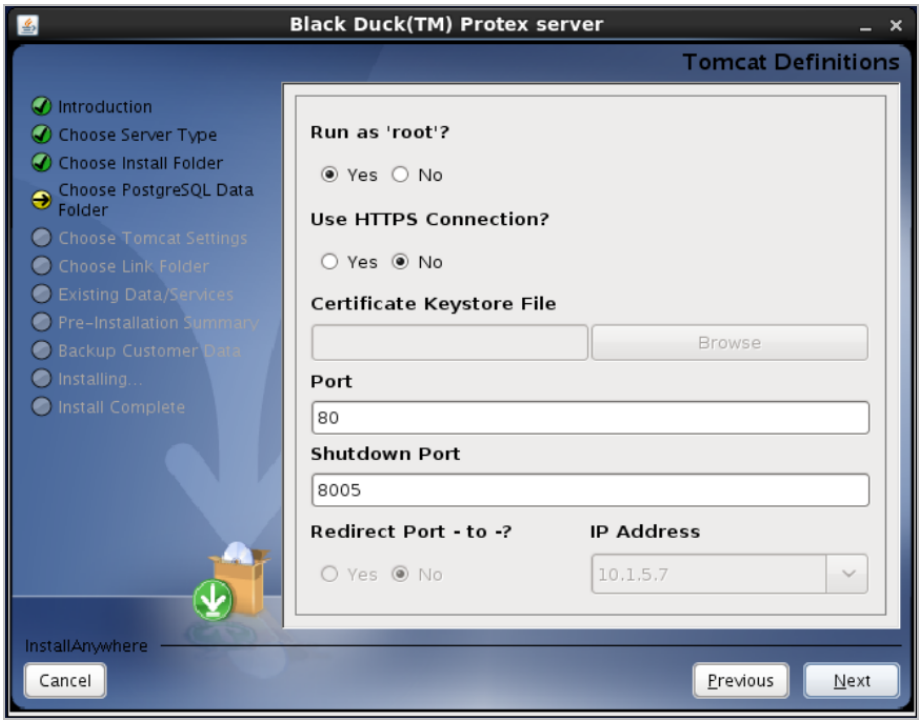
7. On the **Choose PostgreSQL admin home directory** screen, specify the directory for the PostgreSQL admin (`bds-protexip`) and click **Next**. The Protex installer automatically creates the `bds-protexip` user.

Figure 2.6: Server - Choose search index directory



8. In the **Choose search index** screen, specify a directory for the Solr search data and click **Next**.The default location is `/var/lib/bds-protexip/solr`.

Figure 2.7: Server - Tomcat Definitions

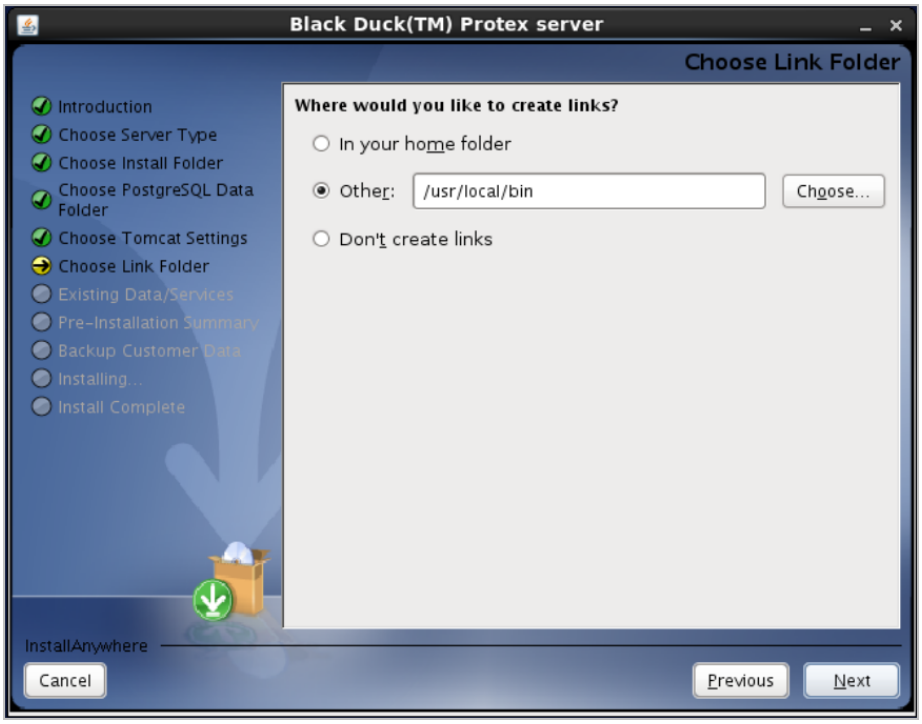


9. In the **Tomcat Definitions** screen, specify the settings to use when running Tomcat. If your company policy prohibits applications from running as root on Linux systems, you have the option of having Tomcat run as the `bds-protexip` user instead. The `bds-protexip` user has all the necessary privileges for database access. Note that this change can only be made at installation time. This option is not available on Windows systems.

   This screen also lets you specify alternate connection details, including running with an HTTPS connection or on another port. Refer to the Protex *System Administrator Guide* for information on how these can be changed post-installation.

10. Click **Next**.

Figure 2.8: Server - Choose Link Folder



11. On the **Choose Link Folder** screen, select a link location and click **Next**. (You can choose not to create a link folder, if desired).

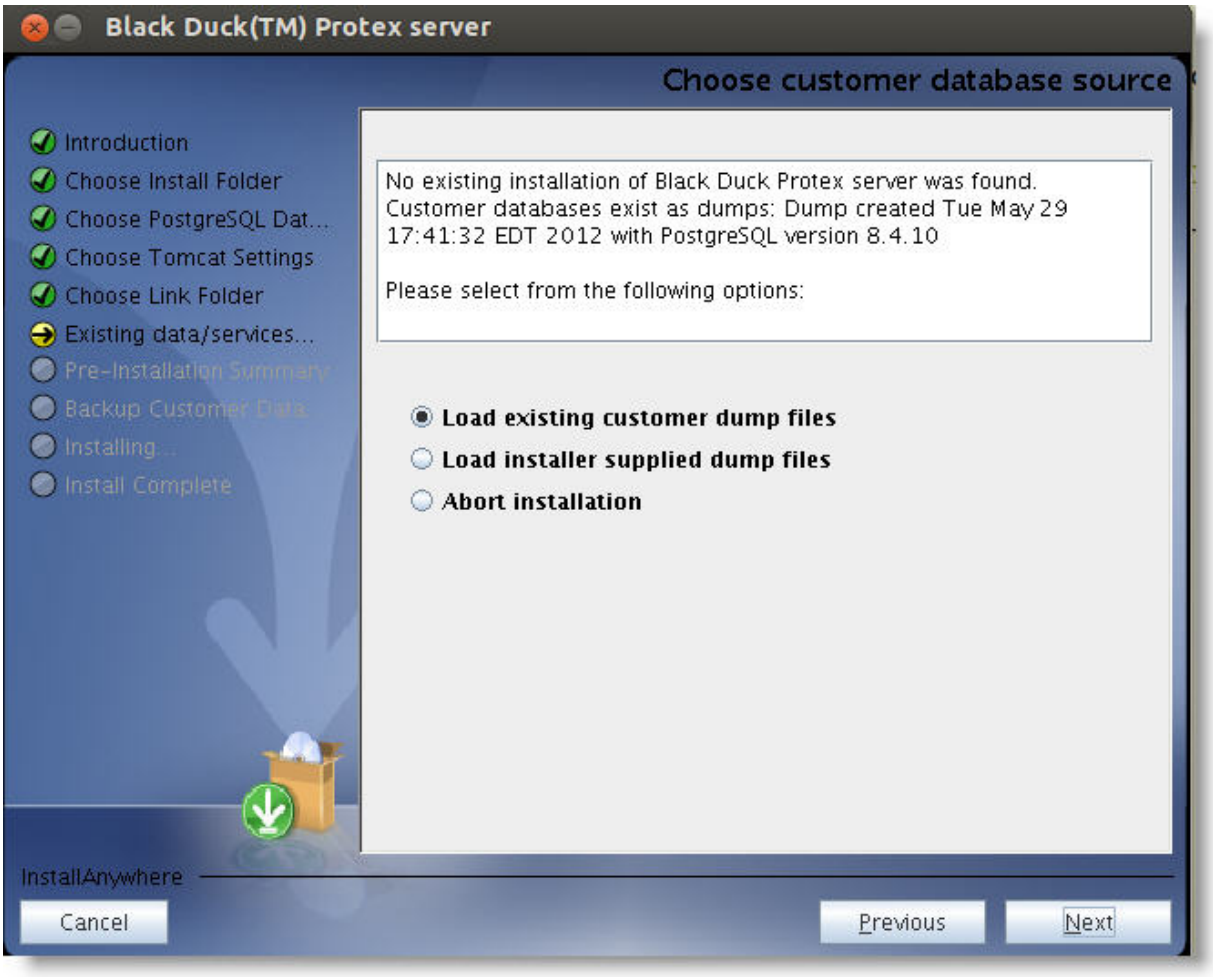
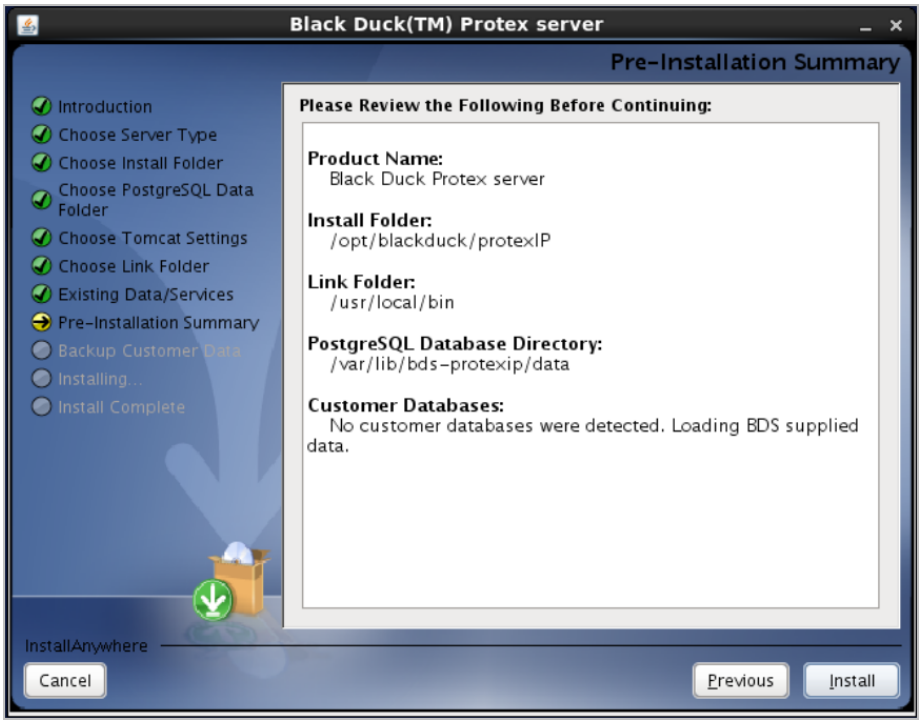


Figure 2.9: GUI Server Choose Customer Data Source

12. The installer checks if this is an upgrade. If so, it asks if you want to load data from the previous install. If not, and the installer does not find a previous database or dump files, it automatically skips to the next screen. Click **Next**.

Figure 2.10: GUI Server Pre-Installation Summary



13. On the **Pre-Installation Summary** screen, verify the installation information. If necessary, click **Previous** to return to a previous screen and edit your responses.
14. Click **Install**. The installation begins and the installer displays its progress.

Server installation can take several hours if this is an upgrade or if you are loading database dump files.

The system notifies you when the installation is done.

Note: You must register your server before you can begin using Protex. See Server Registration on page 36 for details.

2.4.3 Installing the Protex Server Using Console Mode

This section describes how to install the Protex server using console mode on a Linux system.

Note: This installation assumes that your drive is mounted on `/media/PROTEXIP`. Your mount location may be different.

To run the Linux installation:

1. Log in as root on the server.
2. Change your current directory to the media directory:

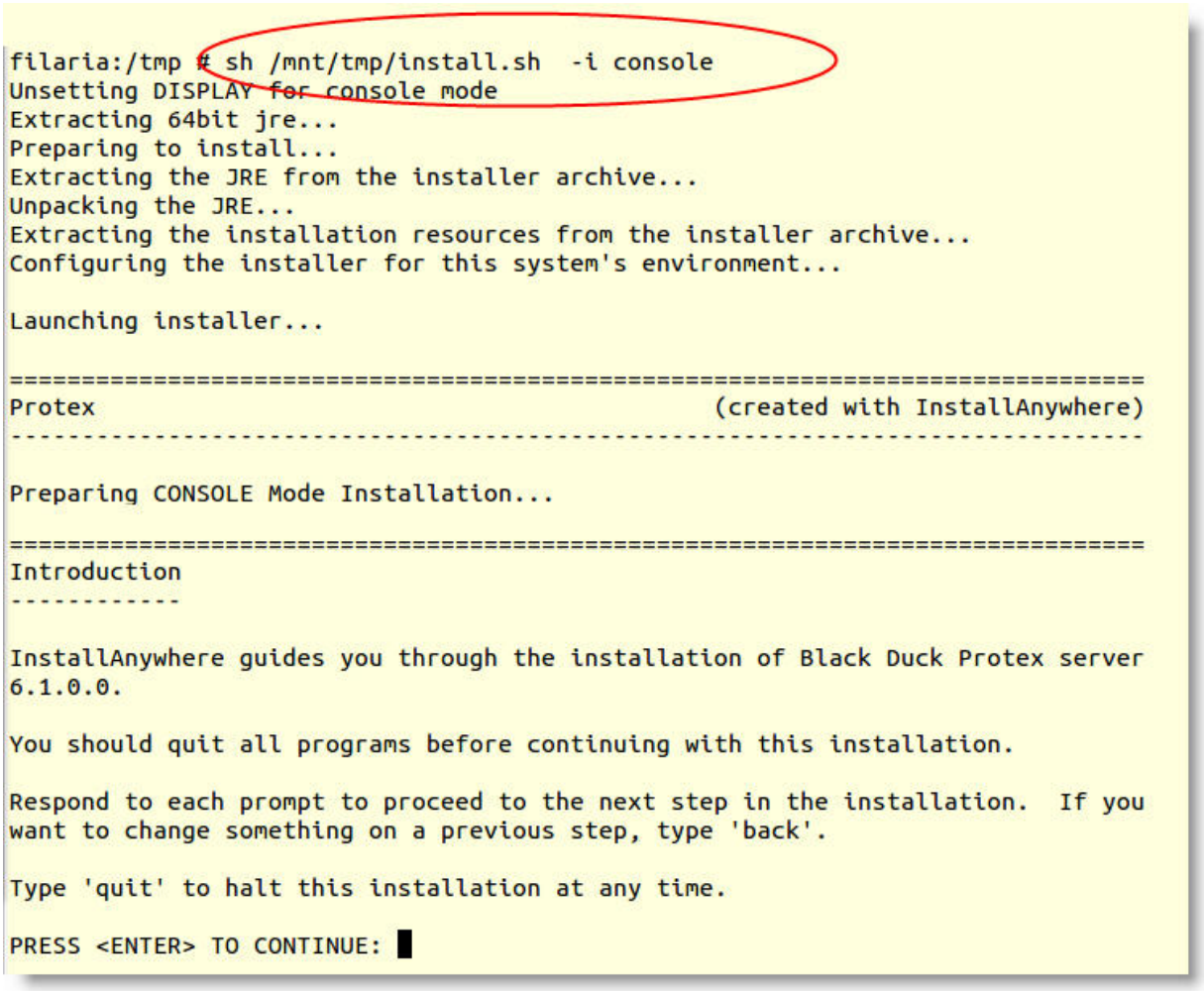
```
cd /media
```

3. Run the installation script.

```
./PROTEXIP/install.sh -i console
```

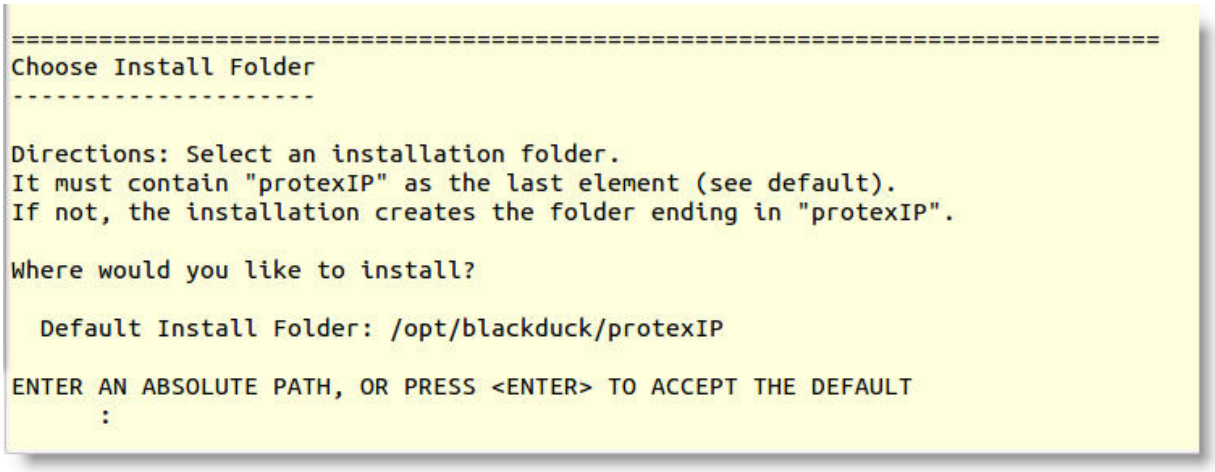
4. The **Prepare Console Mode Installation and Introduction** sections display:

Figure 2.11: Prepare Console Mode and Introduction



5. Press **Enter**. The **Choose Install Folder** section displays:

Figure 2.12: Console Mode Choose Install Folder



6. You can:

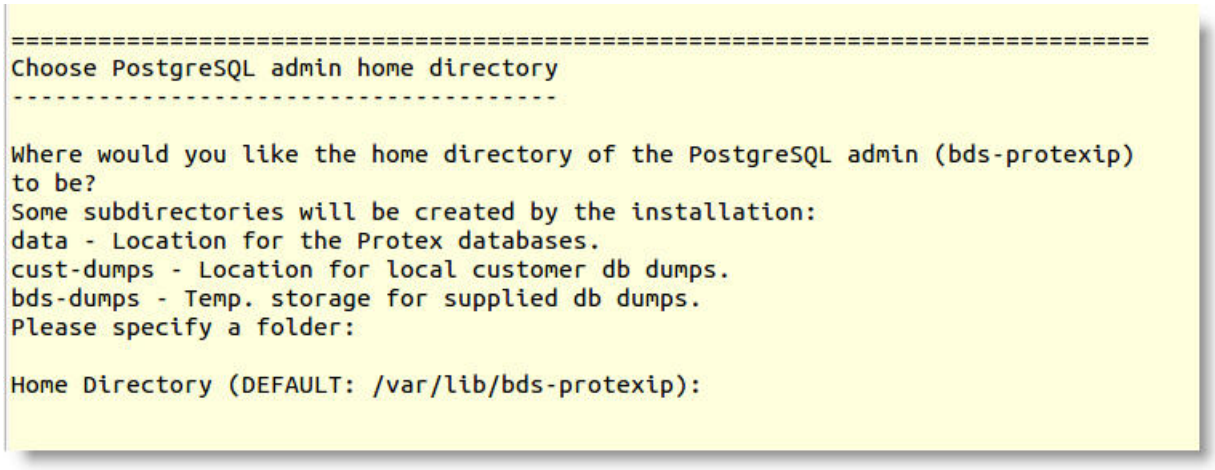
   Enter an absolute path and press **Enter**.

   Or

   Accept the default path and press **Enter**.

7. Enter a value for the link location and press **Enter**. The **Choose PostgreSQL admin home directory** section displays.

Figure 2.13: Console Mode Choose PostgreSQL Admin Directory

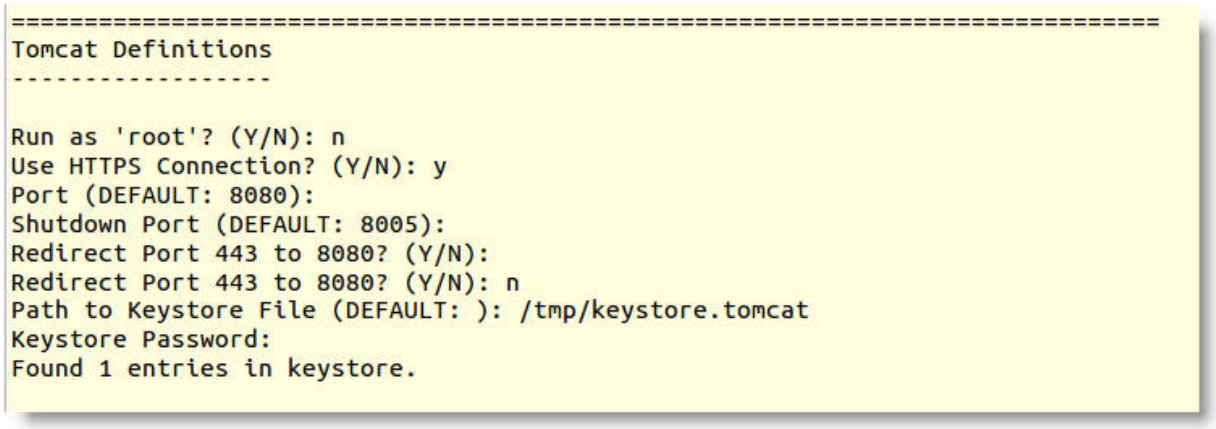


8. Specify a target folder for PostgreSQL and press **Enter**. The **Choose Solr search index directory** section displays.

   If you have less disk space than recommended, the **Recommended Disk Space Warning** screen displays. See Recommended Hardware Requirements - Protex Server on page 14 for disk requirements.

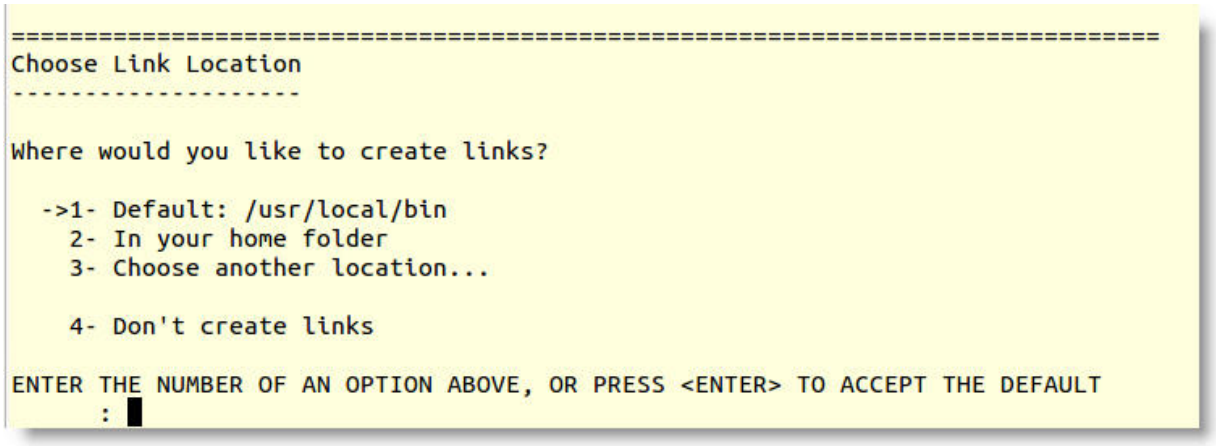
9. Specify a target folder for Solr and press **Enter**. The **Tomcat Definitions** section displays.

Figure 2.14: Console Mode Choose Tomcat Definitions



10. Make your configuration choices for running Tomcat as root, using HTTP or HTTPS. Specify the port numbers Protex can use, pressing **Enter** after each option. The **Choose Link Location** section displays.

Figure 2.15: Console Mode Choose Link Location



11. Enter a value for the link location and press **Enter**. The **Pre-Installation Summary** section displays.

Figure 2.16: Console Mode Pre-Installation Summary

```
================================================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Product Name:
    Black Duck Protex server

Install Folder:
    /opt/blackduck/protexIP

Link Folder:
    /usr/local/bin

PostgreSQL Database Directory:
    /var/lib/bds-protexip/data

Customer Databases:
    Loading BDS supplied databases instead of existing customer database dumps.

PRESS <ENTER> TO CONTINUE:
```

12. Review the information and press **Enter** to start the installation. The **Installing** screen displays the installation progress.

Figure 2.17: Console Mode Installing

```
PRESS <ENTER> TO CONTINUE:

================================================================================
Installing...
-------------
 [==================|==================|==================|==================]
 [------------------|------------------|------------------|------------------]

================================================================================
Installation Complete
---------------------
Congratulations. Black Duck Protex server has been successfully installed to:
/opt/blackduck/protexIP

PRESS <ENTER> TO EXIT THE INSTALLER:
```

Note: Upon completion, you must register the server to use the application. Refer to Server Registration on page 36 for complete details.

This ends Step 2 of the installation. Proceed to Step 3 - Step 3 - Unmounting the Drive on page 36.

2.5 Step 3 - Unmounting the Drive

Note: This example assumes that the external disk drive is mounted under `/media/PROTEXIP`.

To unmount the drive:

To manually mount the drive on your Linux system, unmount it with the following command:

```
umount /media/PROTEXIP
```

On a Windows system, simply unplug the drive from the USB port on your machine.

This ends Phase 3 of the installation. Proceed to Registering the Server on page 37 to register your server prior to use.

2.6 Installing from ISO Images

The Protex installation is distributed on USB drive media. If you have downloaded the installation kit to a server as an ISO image, you can mount that image and follow the same installation procedure.

To install from an ISO image:

1. Mount the ISO using the following command (on Linux):

   ```
   mount -o loop -t iso9660 <FILENAME> <DIR>
   ```

2. On a Windows system, use your favorite freeware tool; for example, *Virtual CloneDrive* to mount the image.

For complete installation details, refer to the Server Installation on page 14 section.

Tip: For Linux users only: you can run the ISO installer as a non-root user.

2.7 Server Registration

To use the server, it must be registered with Black Duck Software. Immediately after installation, you should register the server.

2.7.1 Before You Begin - Registration

Make sure you have the following information available in order to complete the registration. Depending on your requirements, you may need:

- Server registration key.
- Proxy host name (optional).
- Proxy port number (optional).
- Proxy username (optional).
- Proxy password (optional).

2.7.2 Registering the Server

The initial server registration involves two phases, as follows:

- Registration – Activate a formal registration.
- Creation – Create the first user.

To register the server:

1. Using a browser, connect to the server.
2. If locally connected, enter the following URL in the browser:

   ```
   http://localhost
   ```

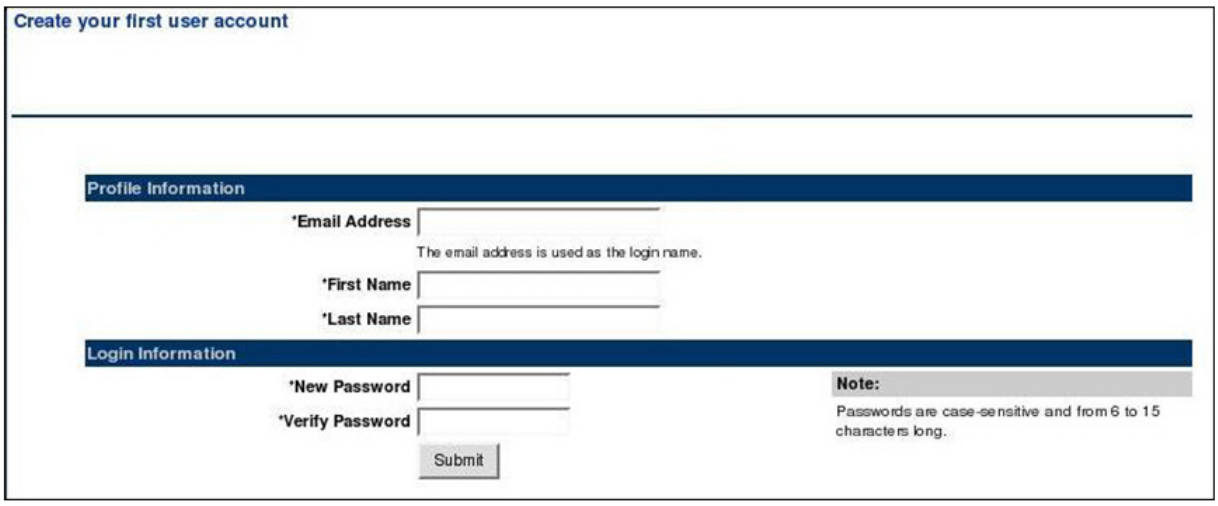
   Or if remotely connected, enter the following URL in the browser:

   ```
   http://<address of server>
   ```

3. Enter the following registration information where applicable. In the Suite interface, navigate to **Administration** > **Registration**.
   - **Registration ID** – Supplied by Black Duck Software.
   - The following fields are optional and are supplied by the local network administrator:
     - **Proxy host name**
     - **Proxy port number**
     - **Proxy username**
     - **Proxy Password**
4. Click **Activate Registration**.

   The browser displays the **Create your first user account** page if the registration key and proxy information are correct. Here is a typical page:

Figure 2.18: Create First User Account



Tip: The system automatically creates a default user account with a username of `admin@blackducksoftware.com` and a password of `blackduckadmin`. The **Create your first user account** page renames this default. If you wish to keep the default, re-enter it on this page. Do not skip this operation.

To create a new user:

Note: Creating a new user deletes the default user and transfers all permissions to the newly created user.

1. 1. Enter the email address.
   2. Enter the user first name.
   3. Enter the user last name.
   4. Enter a password.
   5. Re-enter the password.
   6. Click **Submit**.

2.7.3 Testing Your Server Installation

To verify your Protex installation, complete the following steps:

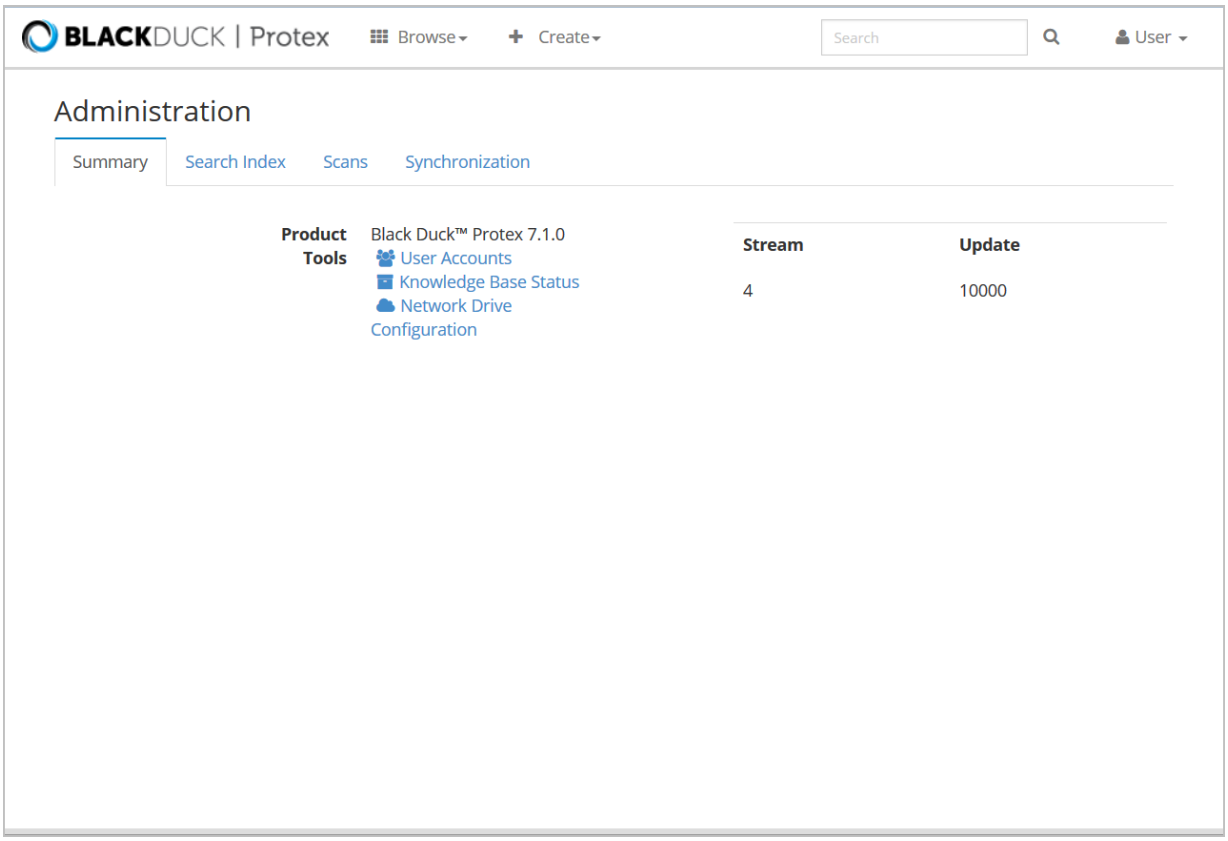
1. Navigate to `http://<hostname>:8080`. If you changed the default port during installation, navigate to `http://<hostname>:<port>`.
2. Log in to Protex using the admin user that you created in the previous step. If you kept the defaults, they are:

   User name = admin@blackducksoftware.com

   Password = blackduckadmin

The Protex **Administration Summary** page opens.

Figure 2.19: Administration Summary page



3. In the **Search** field in the header, enter a search term; for example, `Linux`, and press **Enter**. Protex displays KnowledgeBase components, licenses, and projects that match your query term or terms.
4. You can use the filters on the **Search Results** page to refine your search results.
5. Click the underlined project name to view the **Project Summary** page.
6. From the user name menu, select **Administration**.
7. On the **Administration** > **Summary** page, click **Tools** > **User Accounts**. The Classic user interface opens in a new browser window.

After completing the application server installation and registration, you can begin creating users, assigning roles, configuring analysis settings, and creating projects for code analysis.

Note: There must be at least one user assigned the administrator role. You must create a user with either the manager or project lead role to create a project.

2.7.4 Detailed Product Registration Report

The **Detailed Product Registration Report** shows you how much longer your registration is in effect and displays a warning if you are close to expiration or other license limits.

You can view your product registration information in the Suite interface on the **Administration** >

Registration page. To view the **Detailed Product Registration Report**, select **Detailed Report** from the **Show** menu.

Chapter 3: Client Installation Overview

This section describes how to install the Protex Client software on Linux and Windows systems.

Installing the Protex Client enables you to scan code from your laptop or desktop, and analyze the results. The Protex Client also includes the **File Comparison Tool**. When you run a code scan, Protex accesses the Black Duck KnowledgeBase and application code from the Black Duck server.

This section describes how to install the Protex client on both Windows and Linux systems. The client software should be installed on a different computer than the Protex application server.

The client installation workflow is:

1. Check hardware requirements.
2. Download the installation files.
3. Run the installation.

3.1 Recommended Hardware Requirements - Protex Client

The following minimum hardware configuration is required for a Protex client installation:

- Processor: Pentium 4 (1 GHz)
- RAM: 2 GB
- Storage:
  - 150 MB of hard disk space for the installer download.
  - 200 MB of additional space for the installation.

  For example, if you download the package to drive `C:` and install it on drive `E:`, you need 150 MB of disk space on drive `C:` and 200 MB of disk space on drive `E:`. After the installation, you can delete the download kit from drive `C:`.
  - Additional space on the local system to store the source files to analyze.
- Connectivity: Full internet access is recommended, but not required. Note that the **File Comparison** tool requires internet access.

For additional hardware information, refer to Recommended Project Sizes and Project Size Limitations.

3.2 Operating System Requirements - Protex Client

The Protex client is supported on the following operating systems:

Table 3.1: Protex Operating System Requirements - Client

Operating system	Supported versions
Microsoft Windows	10 Professional and Enterprise
Mac	10.11 (El Capitan)
	10.12 (Sierra)
	10.13 (High Sierra)

The client may work on other distributions, but they are not supported at this time.

Note: Support for the Protex client on Windows XP, Server 2003, and Vista ended July 31, 2015.

3.3 Before You Begin - Client Installation

Before beginning the Protex client installation process, you must:

- Download the installation software package.
- Decide where to install your client files.

3.4 Installing the Client

There are five versions of the Protex client software. Installers are available for the following operating systems:

- Linux (32-bit and 64-bit)
- Mac
- Windows (32-bit and 64-bit)

To install the Protex client software, choose the installer that is appropriate for your operating system, and perform the designated instructions.

Note: 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.

Tip: In Linux, you can run the ISO installer as a non-root user.

Note: You can install Protex client even if you are not a root user. For more information, refer to Installing Protex as a Non-root User on page 21.

3.5 Client Installation on Linux

The Protex client installation on the Linux operating system involves the following steps:

1. Download software.
2. Installation.

Step 1 - Download Software

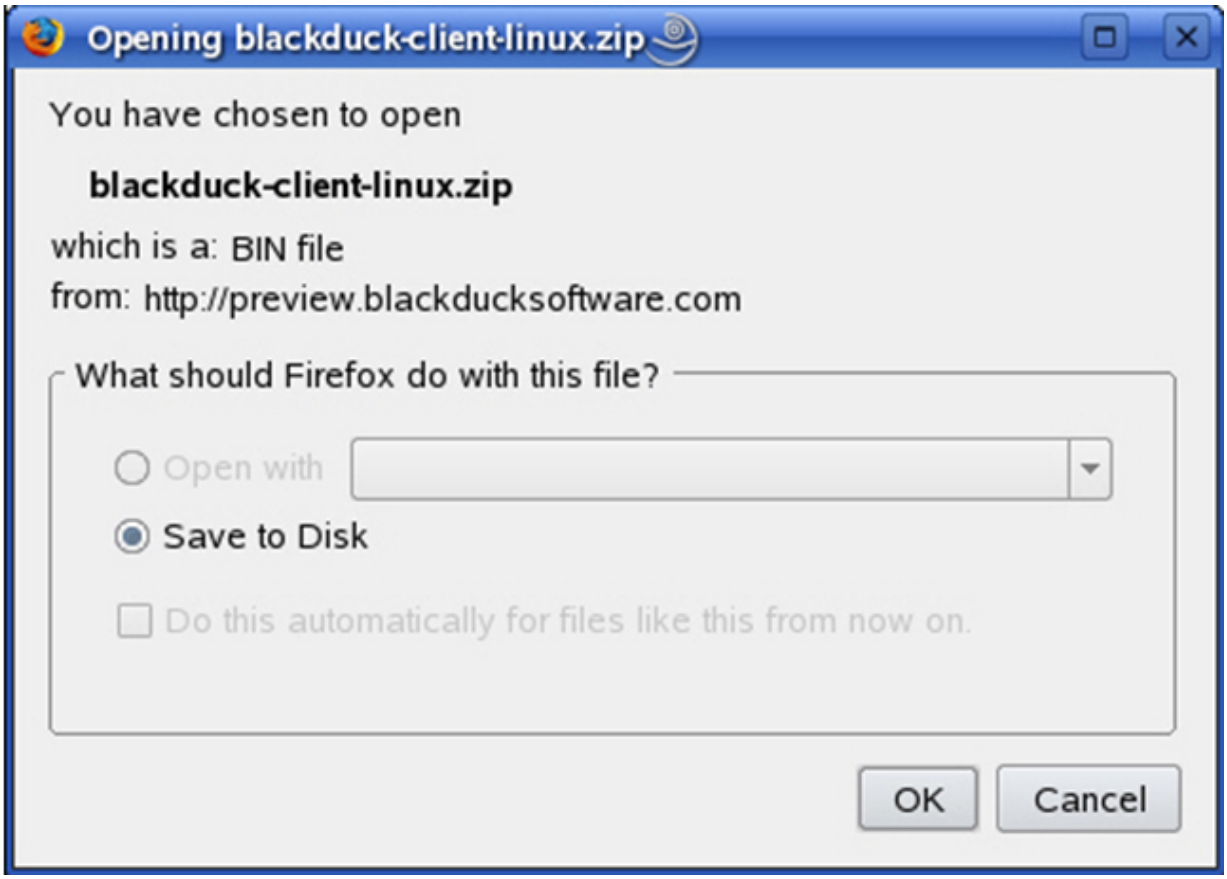
To download the software:

1. Log in to Protex as administrator, using the following username and password:
   - User: `admin@blackducksoftware.com`
   - Password: `blackduckadmin`

   The **Administration** page opens.
2. From the username menu in the Suite interface, select **Tools**. The **Tools** page in the Classic interface opens.
3. On the **Tools** page, click the **Protex Client Software** link. The **Tools** > **Protex Client Software** page opens.
4. Click the appropriate client download link:
   - Download (32-bit Linux)
   - Download (64-bit Linux)

   The **Save to Disk** dialog opens.

Figure 3.1: Client Save to Disk dialog (Linux)



5. Click **OK**. The zip file is saved to the desktop (default).
6. Unzip the saved file to a working directory for the next step.

Step 2 - Installation

To install the Protex client:

1. Log in as root.
2. Open a shell.
3. Enter one of the following commands:

```
sh <PATH>/<ClientFileName>.bin
```

Or:

```
sh <PATH>/<ClientFileName>.bin -i console
```

Or:

```
sh <PATH>/<ClientFileName>.bin -i silent
```

For example, if you are installing the 64-bit client:

```
sh <PATH>/blackduck-client-linux-amd64.bin
```

Or:

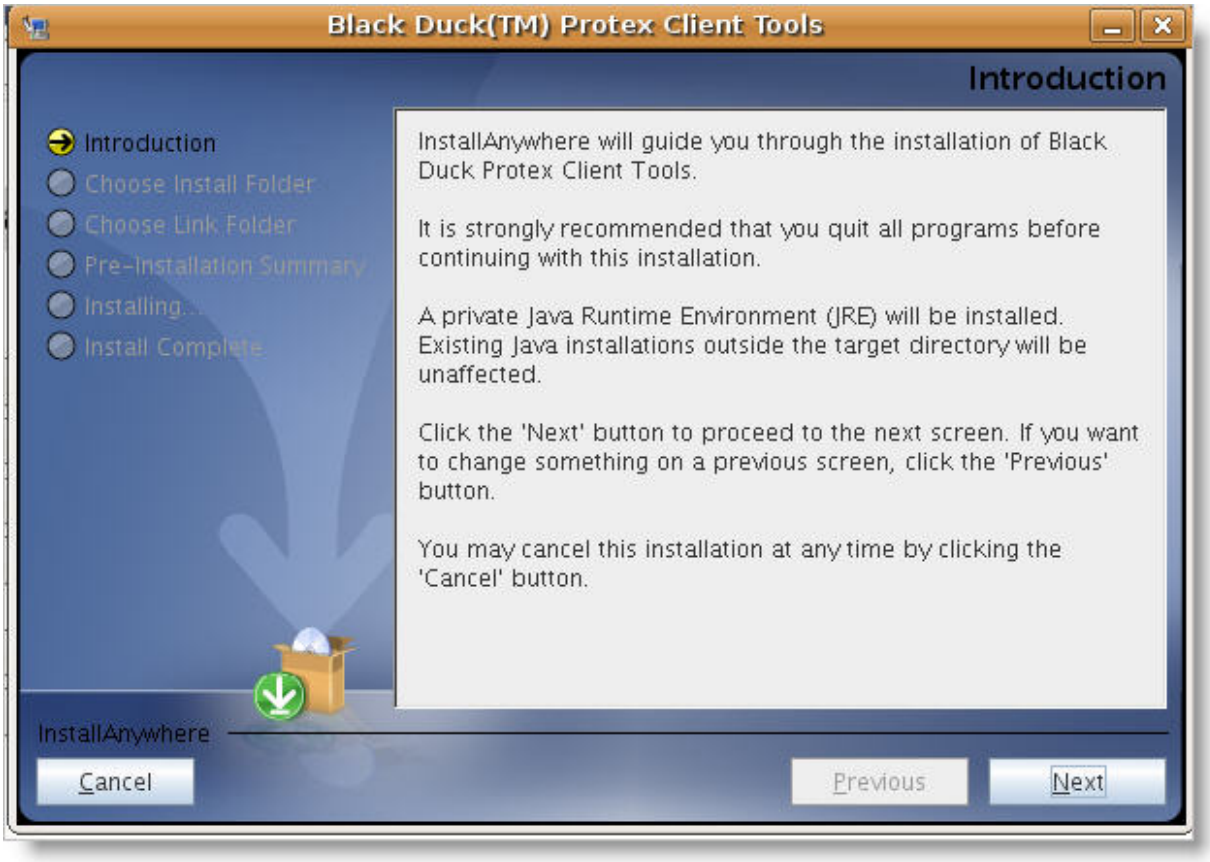
```
sh <PATH>/blackduck-client-linux-amd64.bin -i console
```

Or:

```
sh <PATH>/blackduck-client-linux-amd64.bin -i silent
```

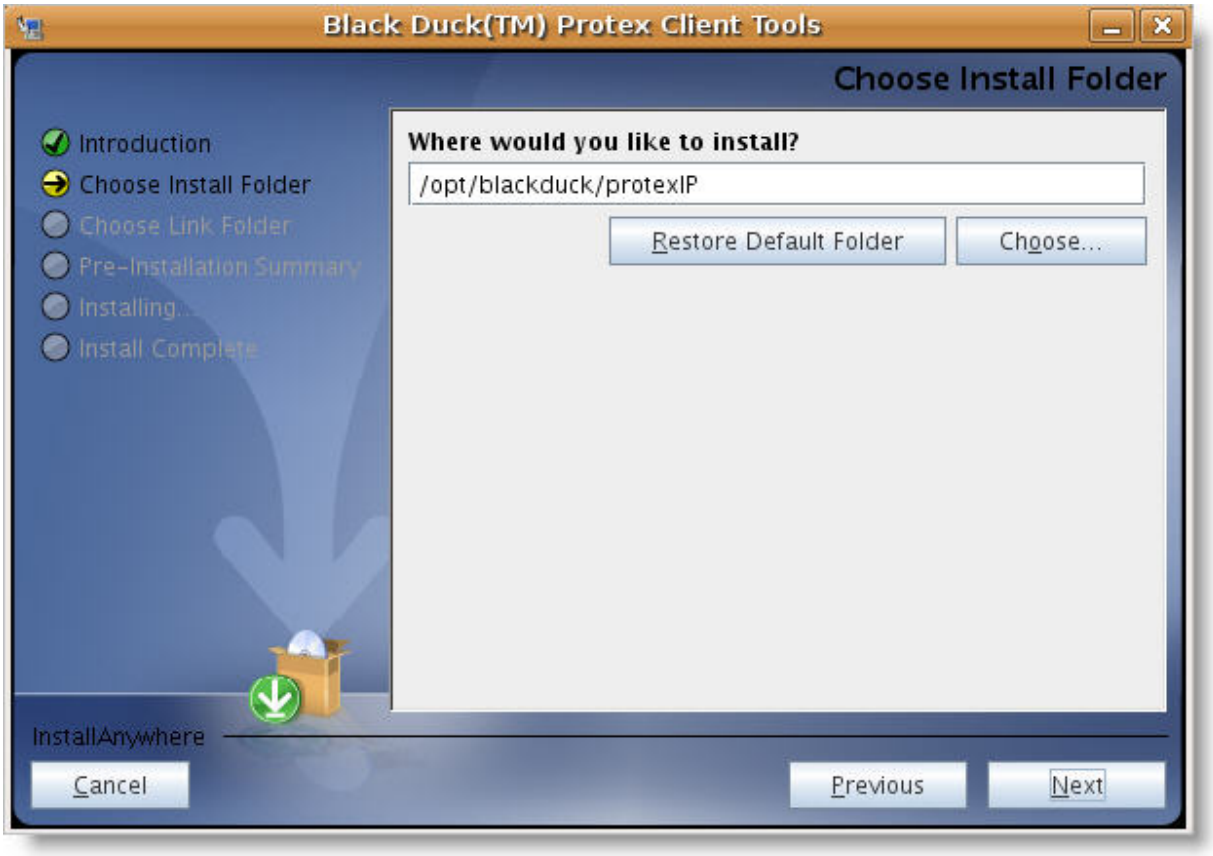
The installer launches.

Figure 3.2: Client Introduction dialog (Linux)



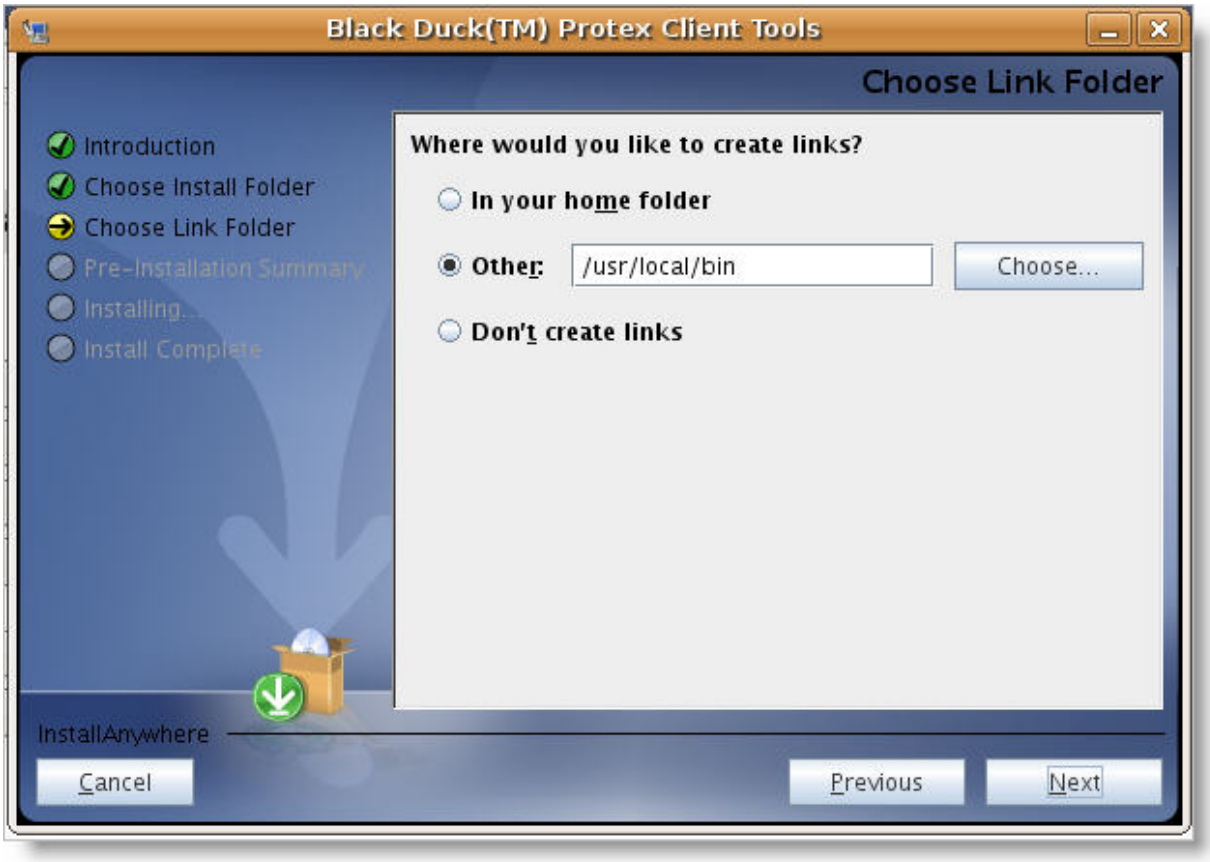
4. Click **Next**.

Figure 3.3: Client Choose Install Folder dialog (Linux)



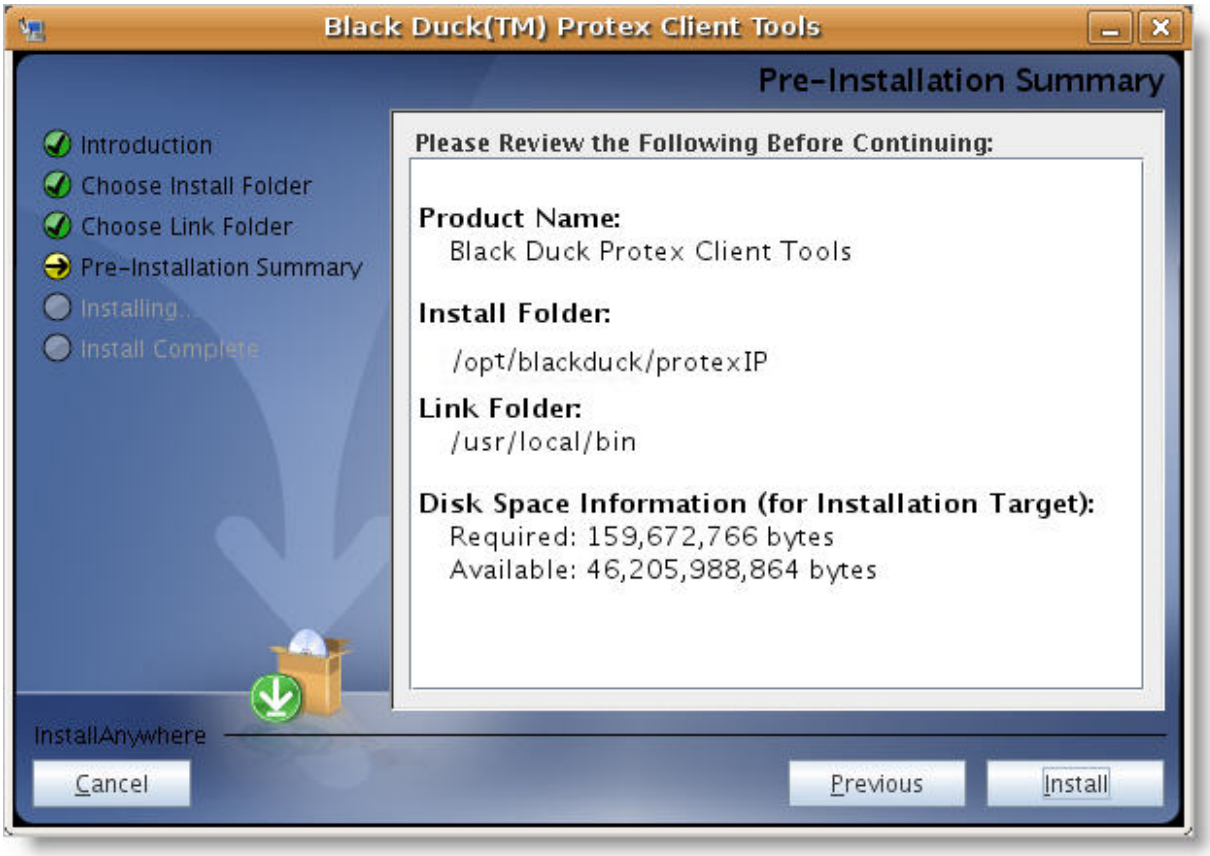
5. On the **Choose Install Folder** screen, specify a directory for the installation. The default directory is `/opt/blackduck/protexIP`. Click **Choose** to browse for a particular directory. Click **Restore Default Folder** to re-establish the original default setting.
6. Click **Next**.

Figure 3.4: Client Choose Link Folder (Linux)



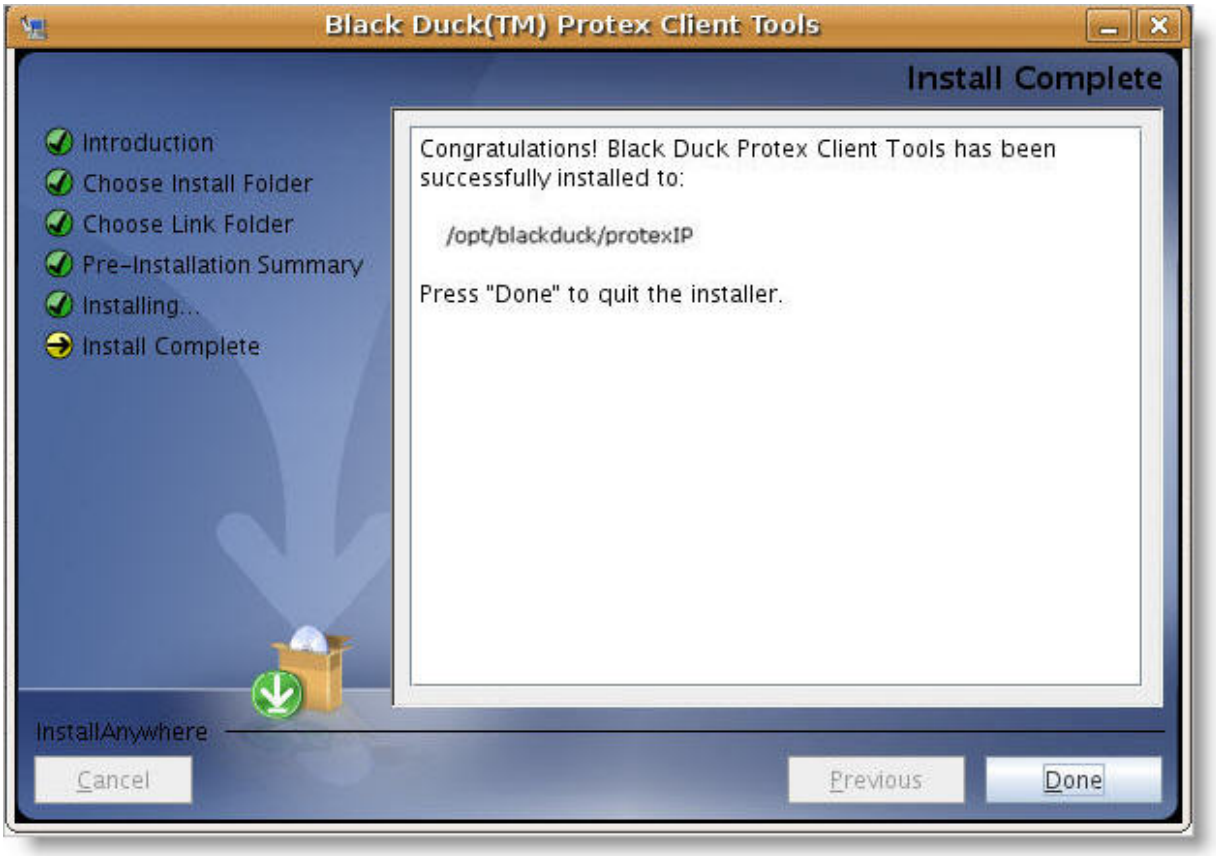
7. On the **Choose Link Folder** screen, select a link location and click **Next**.

Figure 3.5: Client Pre-Installation Summary (Linux)



8. On the **Pre-Installation Summary** screen, click **Install**. The installation begins, and the installer displays a **Progress** screen.

Figure 3.6: Installation Complete dialog (Linux)



9. On the **Installation Complete** screen, click **Done** to exit the installer.

3.6 Client Installation on Mac

The Protex client installation on the Mac operating system involves the following steps:

1. Download software.
2. Installation.

Step 1 - Download Software

Note: You must have cookies enabled. If you have not already enabled cookies, do so now.

To download the software:

1. Log in to Protex.
2. Click the **Tools** link in the upper right of the screen.
3. Select **Tools** > **Download** > **Protex Client Software**. The **Download Client Software** page opens.
4. Select the file `blackduck-client-macosx.zip`, which includes the **MegaByte Estimation Tool**

download link.

5. Click **OK**. The file downloads to your desktop (default setting).

Tip: Save the client software to disk for multiple client installations. This saves time and can be used multiple times as required.

Step 2 - Installation

To install the Protex client on Mac OS:

1. Locate the directory where you saved the zip file.
2. To run the installer, double-click the file (`Blackduck-client-macosx.zip`).

Caution: Do not use the unzip command to extract the installation files as it does not set the permissions correctly. Double-click the zip file or use the *Open* command.

Zip file extraction creates the folder `blackduck-client-macosx` with the following contents:

- `Client.properties`
- `Install`
- `Jssecacerts`
- `ReleaseNotes.txt`

Note: For Mac OS Sierra versions, it is required to run the command `xattr -cr.` (include the period at the end of the command) on the expanded (unzip'd) directory before running the installer. For non-Sierra Mac OS versions, this step is recommended, but not required.

3. Click **Install application**. The following message appears:

```
Warning - "install" can't be opened because it is from an unidentified
developer.
```

4. Click **OK** to dismiss the warning.
5. Go to system preferences (**Apple** menu > **System Preferences**).
6. Click **Security and Privacy**.
7. On the **General** tab, click **Open Anyway** to launch the installation. The following message appears:

```
"install" is an application downloaded from the Internet. Are you sure you
want to open it?
```

8. Click **Open**. The installer launches.
9. Click **Next**.
10. On the **Choose Installation Folder** screen, specify a directory for the installation. The default is the **Applications** folder. Click **Choose** to browse for a particular directory. Click **Restore Default Folder** to re-establish the original default setting.
11. Click **Next**.
12. On the **Choose Alias Folder** screen, select the location for the product icons and click **Next**.

13. On the **Pre-Installation Summary** screen, click **Install**. The installation begins and the installer displays a **Progress** screen.
14. On the **Installation Complete** screen, click **Done** to exit the installer.

3.7 Client Installation on Windows

The Protex client installation on the Windows operating system involves the following steps:

1. Download software.
2. Installation.

Step 1 - Download Software

To download the software:

1. Log in to Protex as administrator using the following username and password credentials:

   ```
   User: admin@blackducksoftware.com
   Password: blackduckadmin
   ```

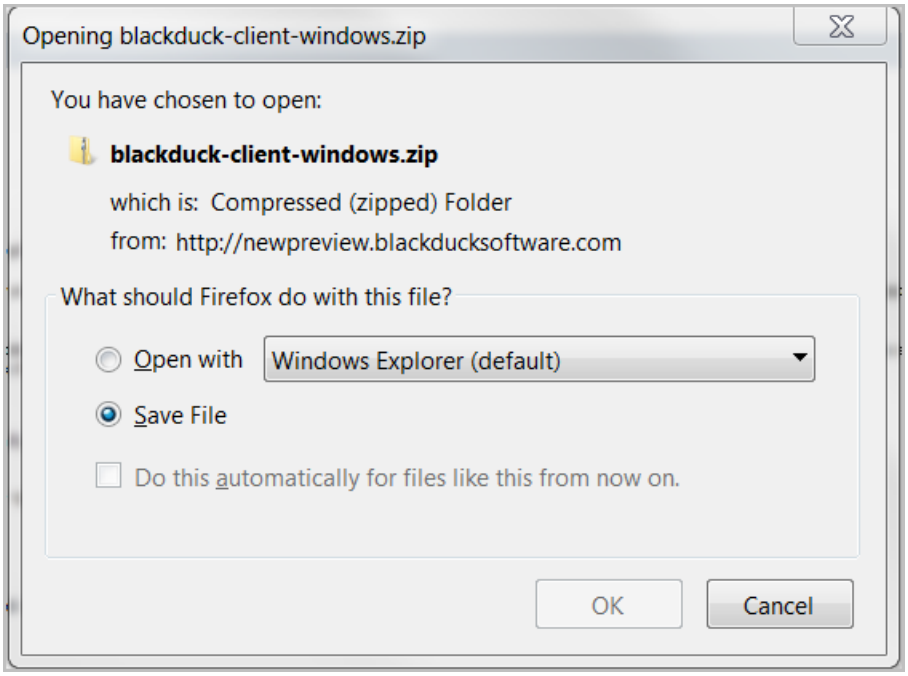
   The **Administration** page opens.

2. From the username menu in the Suite interface, select **Tools**. The **Tools** page in the Classic interface opens.
3. On the **Tools** page, click the **Protex Client Software** link. The **Tools** > **Protex Client Software** page opens.
4. Under **Client Software**, click the appropriate client download link:
   - Download (32-bit Windows)
   - Download (64-bit Windows)

   The `blackduck-client-windows.zip` **Save As** dialog opens.

Note: 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.

Figure 3.7: Client Save to Disk dialog (Windows)



5. Click **OK**. The file downloads to your browser's configured download location.

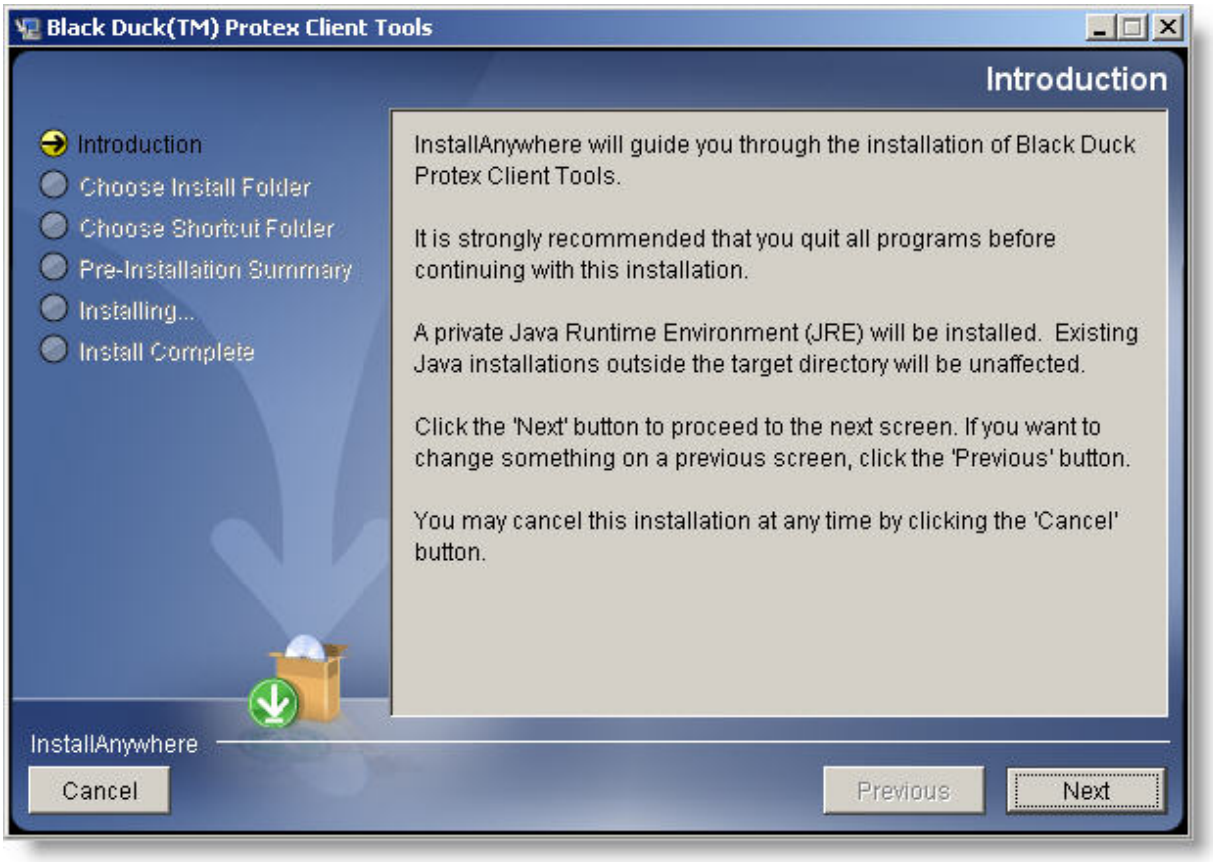
Tip: Save the Client software to disk for multiple Client installations. This saves time and can be used multiple times as required.

Step 2 - Installation

To install the Protex client:

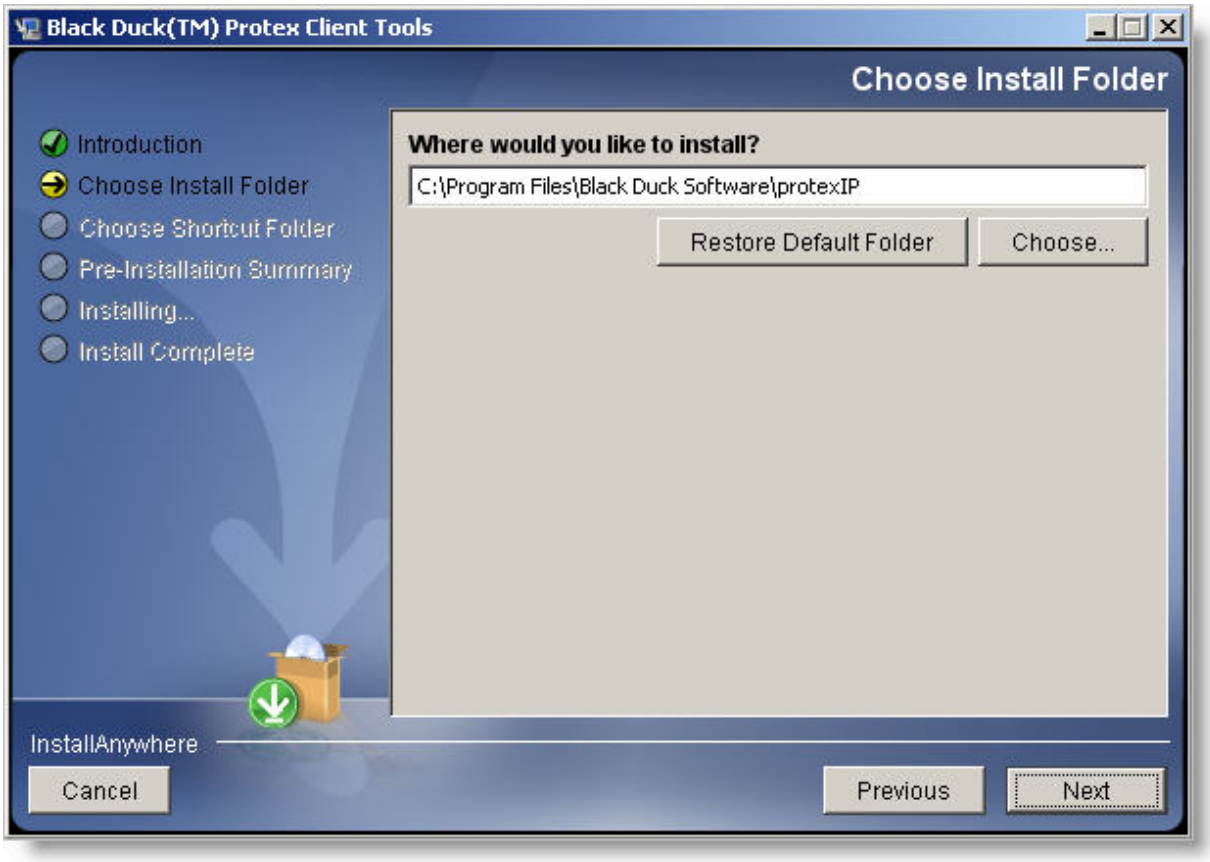
1. Locate the directory where you saved the zip file.
2. Double-click the zip file to extract all files in the zip file.
3. To run the installer, double-click **blackduck-client-windows.exe** in the extracted files. The installer launches.

Figure 3.8: Client Introduction dialog (Windows)



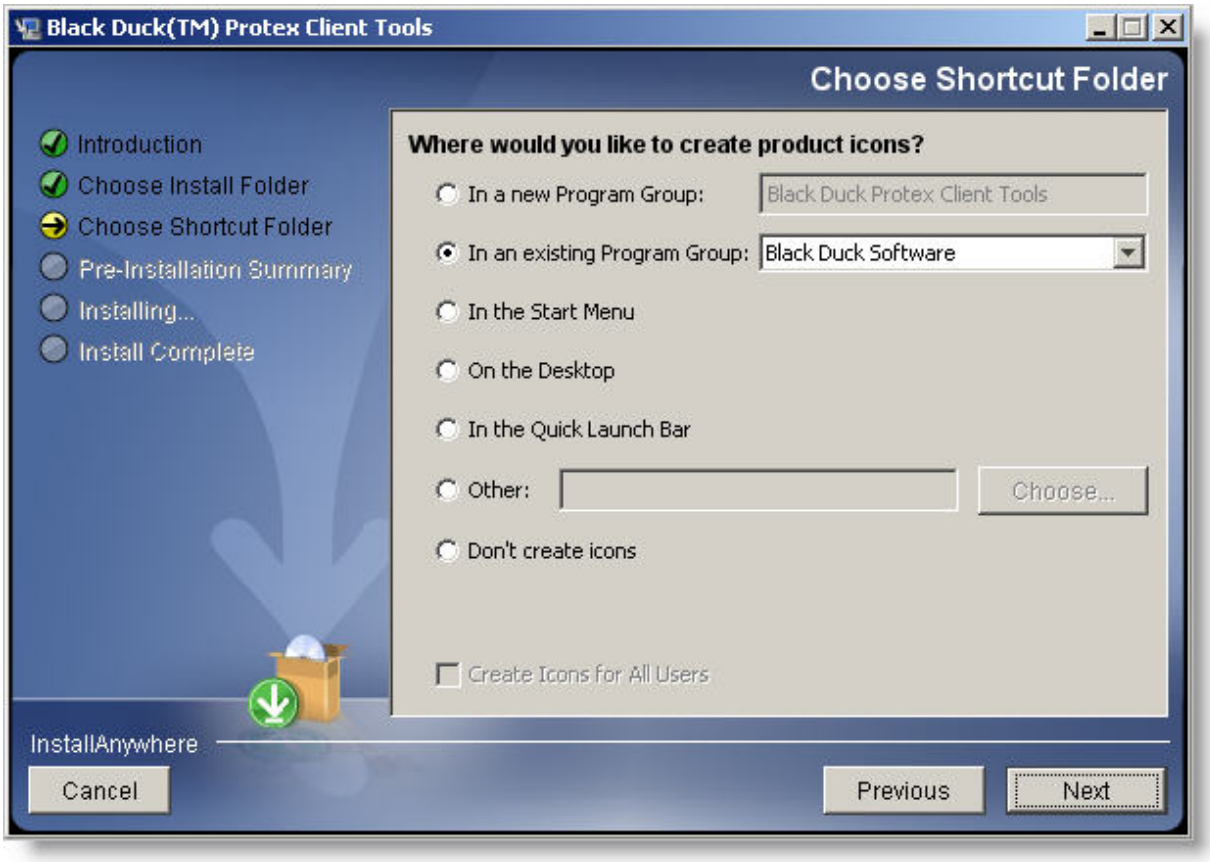
4. Click **Next**.

Figure 3.9: Client Choose Install Folder dialog (Windows)



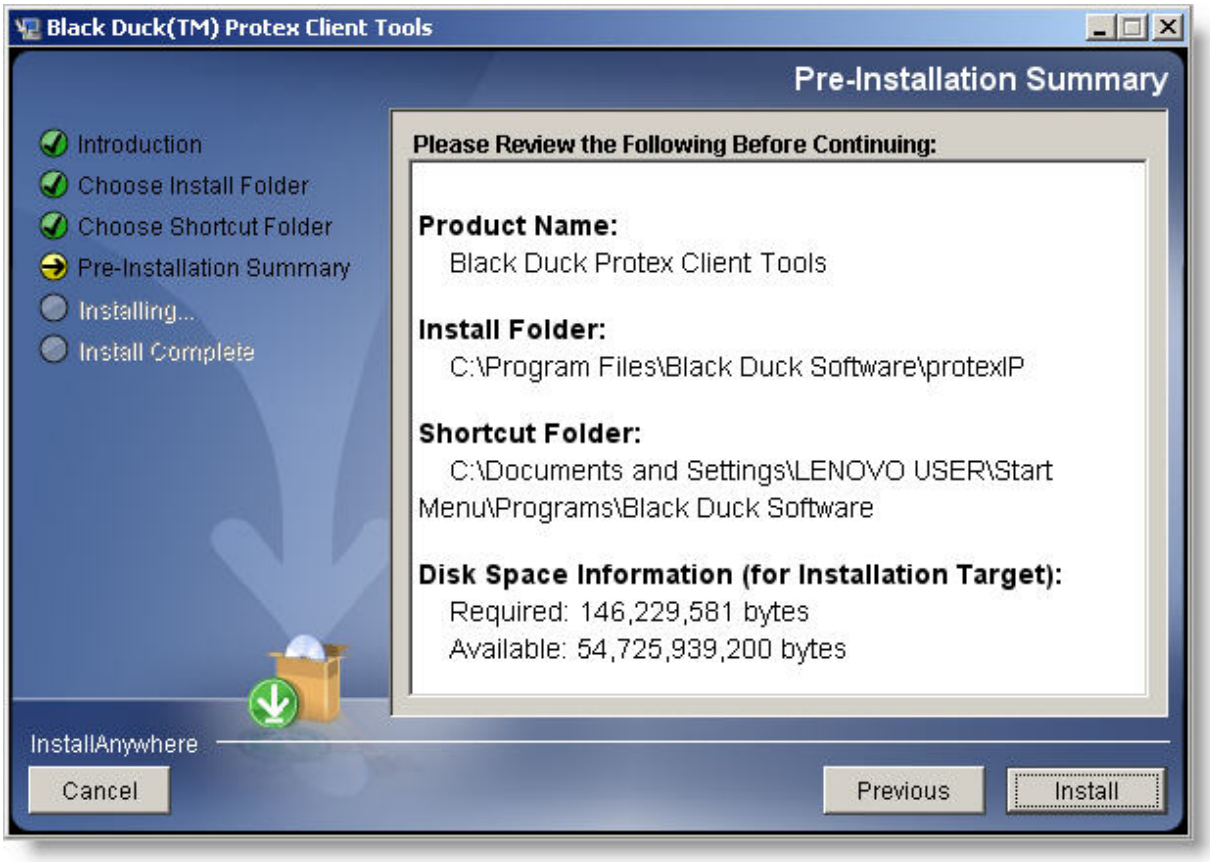
5. On the **Choose Installation Folder** screen, specify a directory for the installation. The default directory is `C:\Program Files\Black Duck Software\protexIP`. Click **Choose** to browse for a particular directory. Click **Restore Default Folder** to re-establish the original default setting.
6. Click **Next**.

Figure 3.10: Client Choose Shortcut Folder dialog (Windows)



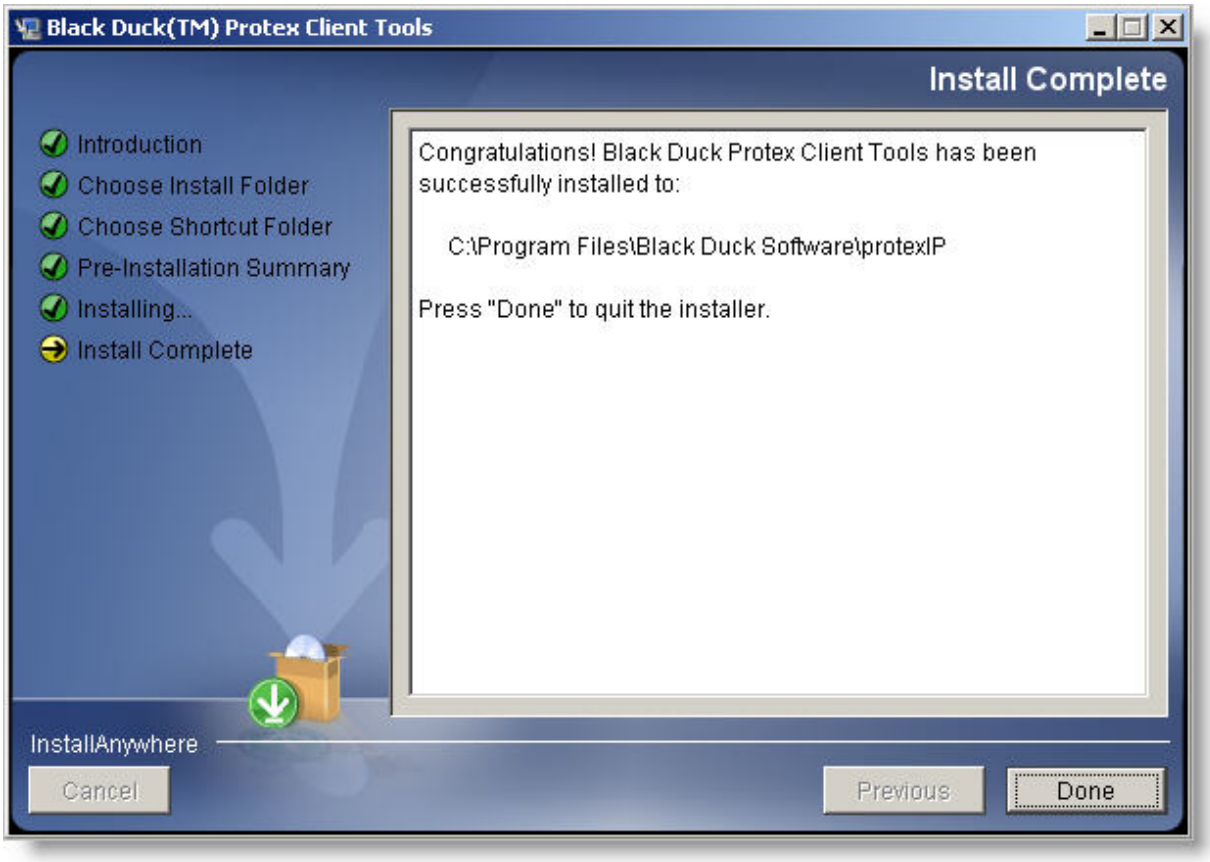
7. On the **Choose Shortcut Folder** screen, select the location for the product icons and click **Next**.

Figure 3.11: Client Pre-Installation Summary (Windows)



8. On the **Pre-Installation Summary** screen, click **Install**. The installation begins and the installer displays a **Progress** screen.

Figure 3.12: Client Installation Complete (Windows)



9. On the **Installation Complete** screen, click **Done** to exit the installer.

3.8 Configuring Server Access to Source Code

This section describes how to set up server access to your source code. Perform this operation after installing the Protex client. The client must be installed to access local source code.

To set up server file access:

1. Log in to Protex.
2. Select **Tools** > **Settings** > **Policy Manager**. The **Policy Manager** page opens.
3. In the **Server File Access** section, select the **Allow Server File Access** check box.
4. Click **Save**.
5. Create a directory on the server named:

```
/home/blackduck
```

By default, the server starts the tree under the root directory of the account (`/root` or `bds-protexip`) that started the server. If you want to include other directories under the root directory, create symbolic links to them. Refer to the Protex *System Administrator Guide* for details on symbolic links.

3.9 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 Suite user interface. Go to **Administration** > **Registration** and under **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**.

3.10 Configuring the Client for SSL

The Protex client and **bdstool** may fail with SSL errors when browsing to a HTTPS URL. You can resolve the problem by adding the Protex server's SSL certificate to the client store of your Protex client's JVM.

A server certificate is required. You can get the server certificate by browsing to the server. You can then use your browser's view and export certificate method. In Firefox and Chrome, browse to the HTTPS URL and export the certificate to a file.

Step 1 - Export the server certificate as a `.CER` file.

Step 2 - Create a backup of the JDK `jssecacerts` file.

Step 3 - Import the certificate (`.CER` file) to the keystore.

Note: Black Duck recommends creating a `jssecacerts` file instead of `cacerts` for your truststore. If a `jssecacerts` file is placed on the server, then the `jssecacerts` file is downloaded when users download the Protex client. The default JRE upgrade behavior from Oracle is to periodically update the `cacerts` file, which overwrites private certificates stored in the file. If a `jssecacerts` file exists in the following directory, Black Duck updates copies the file to the `/cust-dumps` directory before uninstalling and put it back in place after installing the JRE:

```
<INSTALL_DIR>/lib/jre/lib/security/jssecacerts
```

Step 1 - Export the server certificate

To export the server certificate using Chrome, complete the following steps:

1. Launch Chrome.
2. Browse to `https://yourHost.domain.ext`. For example, `https://server.mycompany.com`.
3. Click the padlock icon to left of URL in the address bar.
4. Click the **Connection** tab in the dialog box.
5. Click the **Certificate information** link.
6. In the next dialog box, click the **Details** tab, then click **Copy to File**. The **Certificate Export Wizard** launches.
7. Follow the wizard to export the server certificate to a `*.CER` file.

To export the server certificate using Firefox, complete the following steps:

1. Launch Firefox.
2. Browse to `https://yourHost.domain.ext`. For example, `https://server.mycompany.com`.
3. Click the padlock icon to left of URL in the address bar.
4. In the dialog, click **More Information**.
5. On the **Security** tab, click **View Certificate**.
6. In the **Certificate Viewer** dialog, click the **Details** tab.
7. Click **Export**.

Step 2 - Create a backup of the JDK `jssecacerts` file.

This step requires you to use the Java JDK. You can perform this step on the client computer or on a different computer than the one where the client is located.

1. Locate the client's keystore. This file is a `jssecacerts` file.

   On Linux - `/opt/blackduck/protexIP/lib/jre/lib/security`

   On Windows 7 - `C:\Program Files (x86)\Black Duck Software\protexIP\lib\jre\lib\security`

2. Make a backup of the `jssecacerts` file.
3. If you are on a different computer than the client, move the original file to the computer with the JDK.
4. Copy the `*.CER` file to the computer with the JDK.

Step 3 - Import the certificate (`.CER` file) to the keystore (`jssecacerts` file)

In this step, use the **keytool** utility of the JDK to import the certificate into the keystore.

Note: Black Duck recommends creating a `jssecacerts` file instead of `cacerts` for your truststore.

1. Run the following, replacing the `aliasName` within the brackets with the name you want to use.

   ```
   keytool -import -alias
   {aliasName}
   -keystore jssecacerts -trustcacerts -file
   {certificate.CER}
   ```

   For example:

   ```
   keytool -import -alias blackduck -keystore jssecacerts -trustcacerts -file
   blackduck.CER
   ```

2. When prompted, enter the password: *changeit*.

   Note: Run the **keytool** in the JDK `bin` directory with the `jssecacerts` file and `*.CER` file temporarily placed in the `bin` directory. This eliminates the need to use fully qualified paths for the files. You can then delete or move your `jssecacerts` file and `*.CER` file.

3. You can confirm the certificate was imported by running the **keytool** utility.
4. Finally, overwrite the client JRE's original `cacerts` file with your modified `jssecacerts` file.
5. Stop the client.
6. Run the following:

   ```
   keytool -list -v -keystore jssecacerts -alias {yourAlias}
   ```

   For example,

   ```
   keytool -list -v -keystore jssecacerts -alias blackduck
   ```

7. Move the keystore file back into the `jre/lib/security` directory of the JRE the client is using. This should be the same as its original location.
8. Restart the client.

Note: Note that the URL domain the client uses to connect to the server must be the same as exists in the certificate. For example if the certificate uses `daffyduck.blackducksoftware.com`, your server URL must be `https://daffyduck.blackducksoftware.com`. You cannot use `https://daffyduck/` or the IP address. This can cause a secondary issue. If the servers are on an internal network and DNS cannot translate the hostname to its IP, you must modify the client computer's hosts file. Make an entry in the hosts file with the IP and hostname of the server, matching the format in the certificate. Finally, remember to use HTTPS in the server URL when using the client configuration tool.

Now when you run **bdstool** or the client you should be able to connect to the Protex server using HTTPS.

Chapter 4: Upgrading Protex

Keeping your Protex system up-to-date keeps your software updated with the latest features and bug fixes, and keeps your Black Duck KnowledgeBase updated with the latest information about open source projects.

There are two ways to update your Protex system: an online update, or using the installation media for a new release. For instructions on managing online updates, refer to the *System Administrator Guide*.

Beginning with Protex 7.1, Black Duck separates software upgrades and KnowledgeBase updates into separate streams. The allows you to keep your KnowledgeBase up-to-date while you test software updates.

4.1 Updating the Black Duck KnowledgeBase

Black Duck Software provides regular updates to the Black Duck KnowledgeBase (KB) to incorporate information about new or changed licenses and new open source projects. Your annual support subscription ensures that you receive these regular KnowledgeBase updates. It is important to install these updates as they become available, so that you have the most accurate and up-to-date information.

Update the KnowledgeBase through the Protex user interface. In the Classic interface, go to **Tools** > **Admin Center** > **Update Status**. You can install updates manually, or configure Protex to automatically download and install KnowledgeBase updates. For more information about updating the KnowledgeBase, refer to the *System Administrator Guide*.

Note: During KnowledgeBase updates, you cannot perform identification or review. The **Identify** and **Review** areas in the Classic interface are disabled during KnowledgeBase updates.

4.2 Upgrading the Protex Server

The process of upgrading a Protex server from the installation media is very similar to a Protex installation. The installer automatically recognizes your existing server and migrates your data to the new version. However, there are several things to keep in mind:

- Upgrading from media supports upgrading from two major versions back from the current version. For example, the Protex 7.0 media supports upgrading from Protex 6.3 or 6.4.
- Read the Protex *Release Notes* prior to installing a new version. This details the changes in the new version.
- When upgrading from a previous version of Protex, the installer uses the existing directory structure and does not ask for new locations for the application or database servers. To change these, you must

first uninstall the product, and then run the installation program.

- At the beginning of an upgrade, you have the option of deleting the data stored in your database. This may be useful if you have data in a backup file that you intend to restore into the new database. Otherwise, always keep the existing databases, as they include all your users, projects, custom components, and identifications.
- During an upgrade, parts of the system are unavailable. For example, the **Identification** and **Review** tabs are blocked during an upgrade and you cannot create new projects until the upgrade completes. A message in the header of the disabled features indicates that an upgrade is currently underway.
- A server upgrade may include database schema changes, logic improvements, policy changes, and KnowledgeBase updates. You may want to re-analyze your active projects to take advantage of these changes. It is likely that Protex makes new discoveries requiring identification.

Caution: After upgrading, be sure to take a new backup of your Protex system. The database schema often changes between versions, and previous backup files cannot be applied to the new Protex databases. See the Protex *System Administrator Guide* for information about backing up your databases.

4.3 Upgrading the Protex Client

As a best practice, your Protex client version should match your Protex server version to take advantage of the most recent upgrades. However, some Protex upgrades do not require upgrading the Protex client, as the server upgrades are backwards compatible with older versions of the client. Consult the *Protex Release Notes* for more information about whether client upgrades are required for a particular release.

If your Protex client version does not match your Protex server version, a message similar to the following displays:

```
Warning: Version x.x.x client tools are available from the server,
please download them.
```

This is an informational message. If your client version is actually incompatible with your Protex server version, you will receive an error message and you must upgrade your clients, as a scan fails.

Note: Black Duck Software recommends creating a `jssecacerts` file instead of `cacerts` for your truststore. If a `jssecacerts` file is placed on the server, then the `jssecacerts` file is downloaded when users download the Protex client. The default JRE upgrade behavior from Oracle is to periodically update the `cacerts` file, which would overwrite any private certificates stored in the file. If a `jssecacerts` file exists in the following directory, the Black Duck update copies the file to the cust-dumps directory before uninstalling and puts it back in place after installing the JRE:

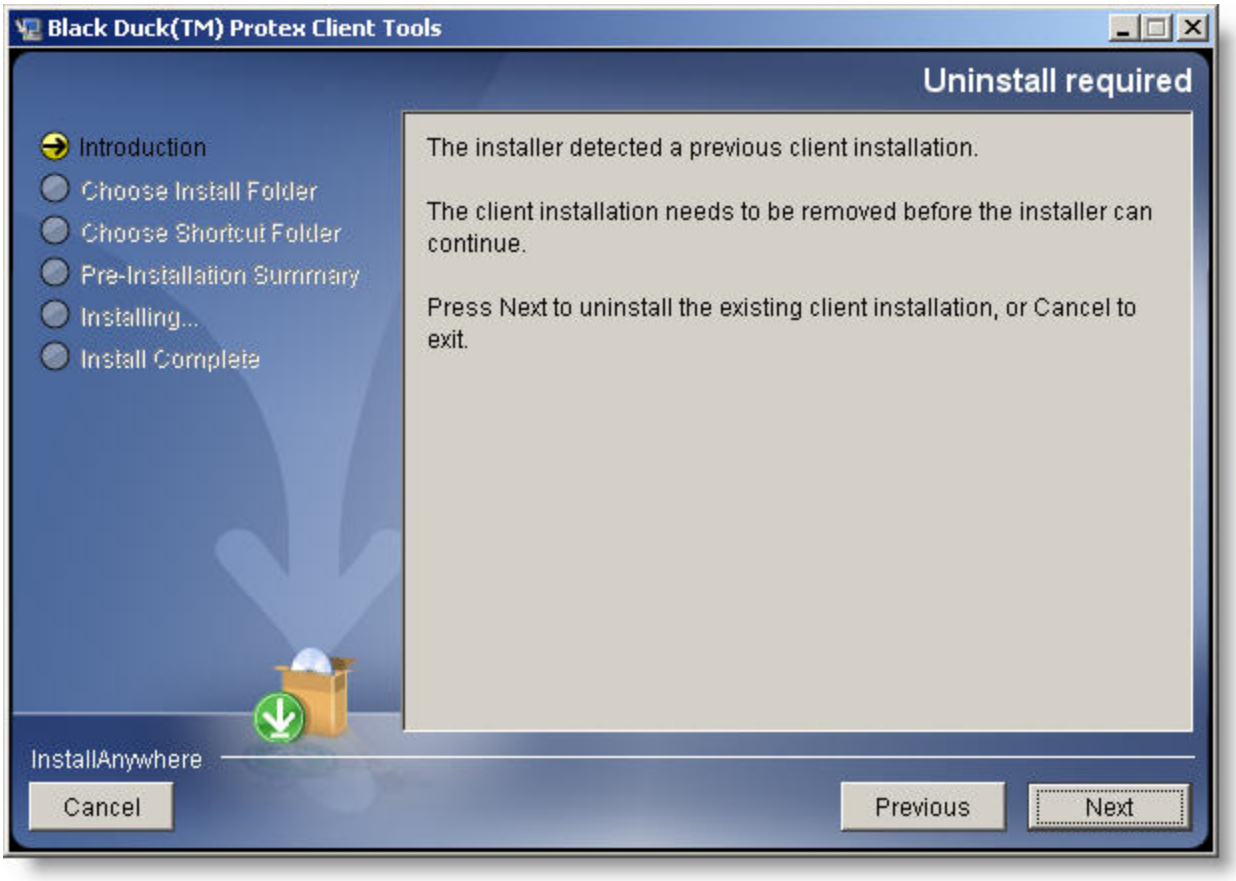
```
<INSTALL_DIR>/lib/jre/lib/security/jssecacerts
```

Custom certificates are preserved during an update only if they are stored in a `jssecacerts` file.

Client upgrades are handled the same way as client installation. When you download and run the client software, the system detects if a previous version is installed. If so, the client installer uninstalls the old version before proceeding.

Tip: During an online update, changes to `downloads/client/client.properties` are copied to `config/client.properties`, overwriting any custom configuration settings that you have specified for your client. For instructions on how to configure an override file to preserve your custom settings, see Configuring Default Client Settings.

Figure 4.1: Client Upgrade



Note: Your client and server software must be the same version. The system tells you if you need to upgrade your client to match the server.

4.4 Debugging and Troubleshooting

As a best practice, after an upgrade you should encourage Protex users to clear their browser cache to ensure that old versions of user interface pages and JavaScript are not being applied to Protex.

If you are using Protex integrations plug-ins, you should check to see if there are updated versions of the plug-in available. Changes to the APIs, schema, and SDK versions can require updated versions of the integration plug-ins.

For specific troubleshooting questions, contact Black Duck Software Customer Support. For contact information, refer to Customer Support on page 6 in the preface of this manual.

4.5 Recovering a Protex Server

If your system has a catastrophic failure (or you are building a new server), you can call Black Duck customer support for assistance. They can provide you with an FTP account so you can download the latest installation image of Protex. This image contains cumulative KnowledgeBase updates and software changes to keep your system current and updated. This makes rebuilding and restoring your system easier than starting from scratch.

Chapter 5: Uninstalling Protex

Both the Protex Server and Protex Client installer include an un-installation program that you can run for system cleanup. This program is included in the installation package.

5.1 Un-installing the Protex Server

This section details how to remove the Protex server installation. Everything you need for the un-installation is already on the system.

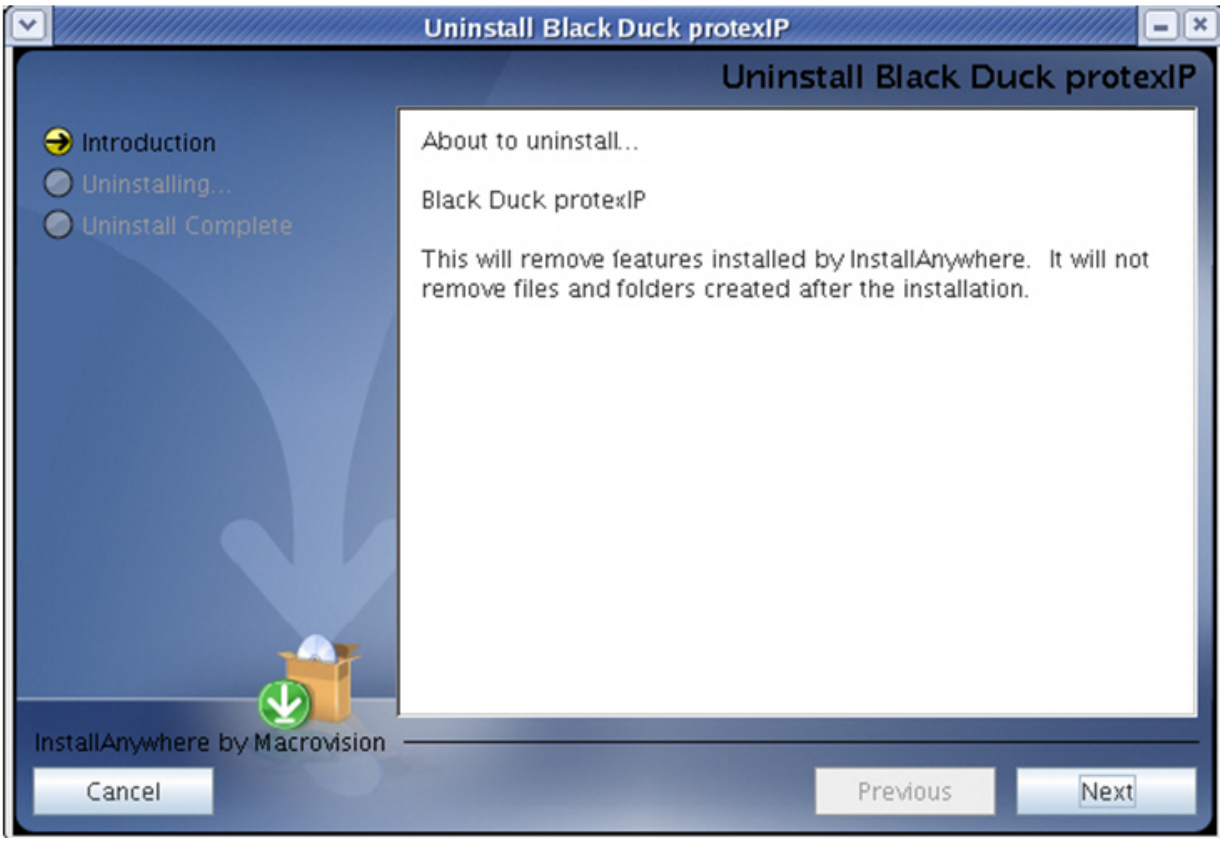
To uninstall the Protex server:

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

   ```
   /opt/blackduck/protexIP/uninstall/uninstall_protexIP
   ```

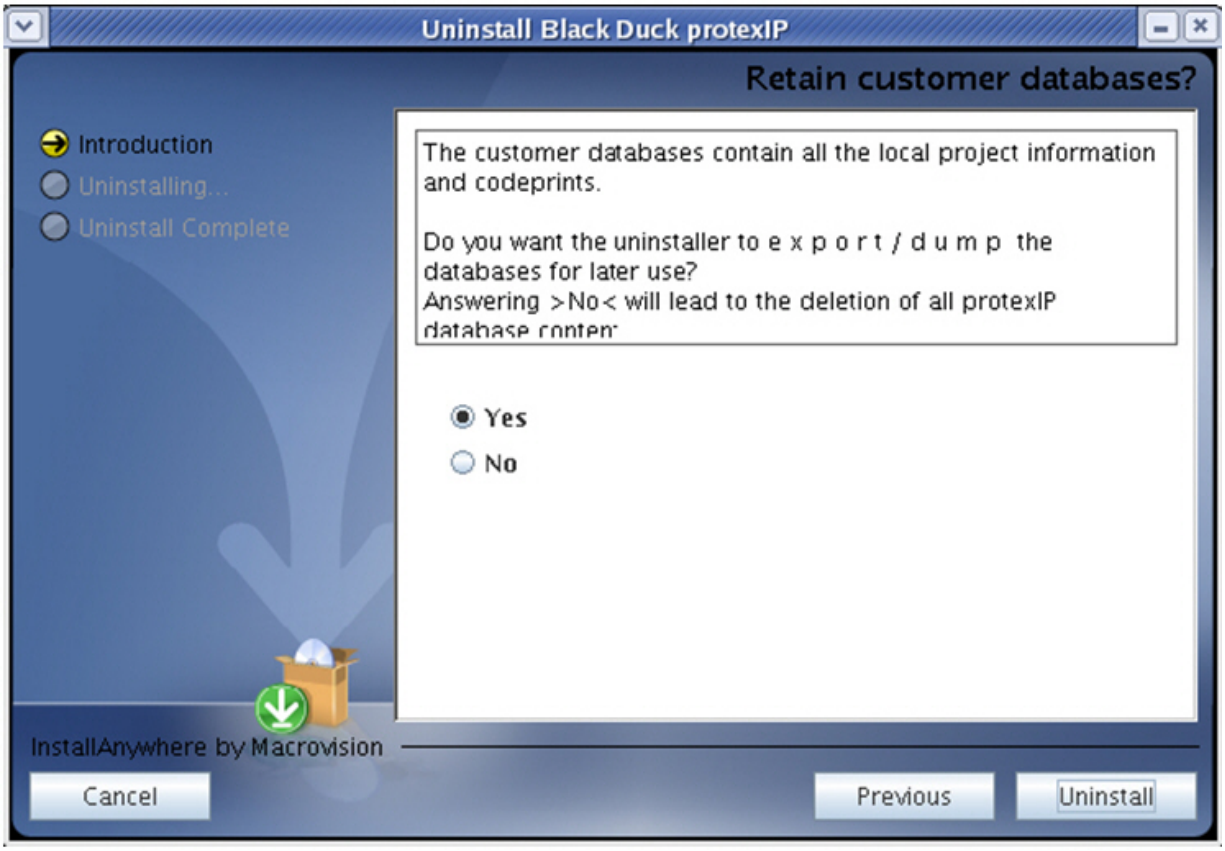
   The **Uninstall Black Duck Protex** screen opens.

Figure 5.1: Un-Install dialog



3. Click **Next**. The **Retain Customer Databases** screen opens.

Figure 5.2: Retain Customer Database dialog



4. Choose **Yes** to save your databases; choose **No** to delete them.
5. Click **Uninstall** and the operation begins.

When the operation completes, you are notified that you have successfully completed the uninstallation.

5.2 Uninstalling the Client Application

There is an un-installation program that you can run for system cleanup. It is included in the installation package.

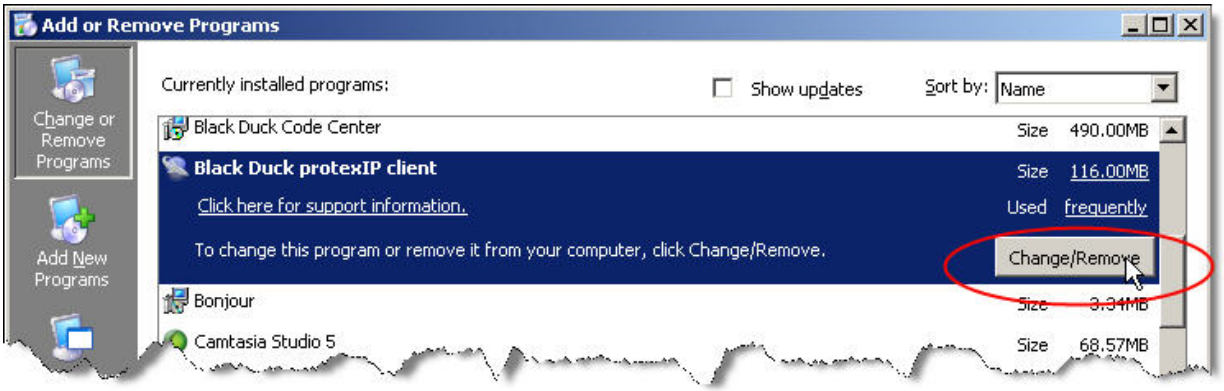
To uninstall the client on Mac OSX:

1. Go to **Applications** > **Protex IP** > **Uninstall**.
2. Click the **Uninstall_protexIP** icon to launch the uninstall program.
3. On the Introduction screen, click **Uninstall**.
4. On the Uninstall Complete screen, click **Done**.

To uninstall the client on Windows:

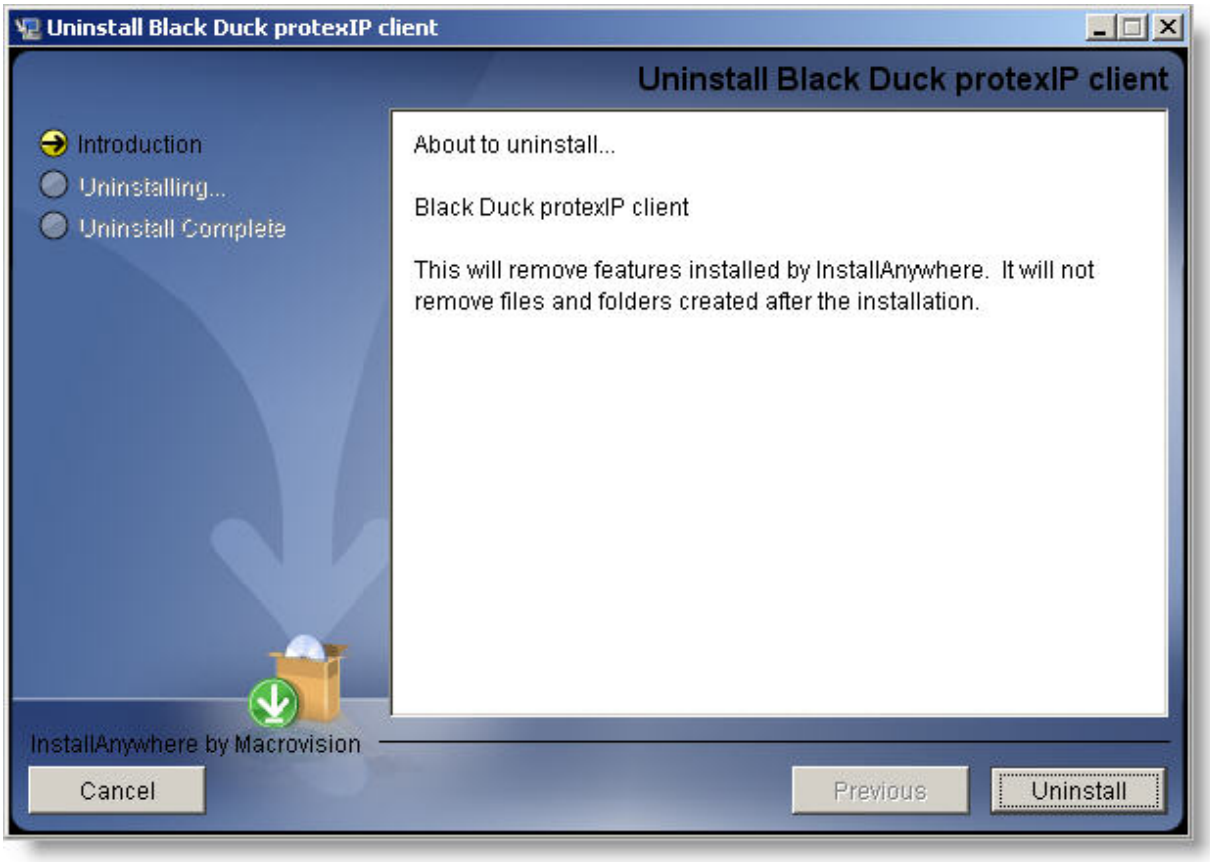
1. From the Windows Start menu, select **Control Panel**. The Control Panel opens.
2. Click **Add or Remove Programs**. The Add or Remove dialog opens.
3. Select **Black Duck protexIP** or **Black Duck Protex** from the list of programs. The **Change/Remove** button displays.

Figure 5.3: Change/Remove button



4. Click **Change/Remove**. The system displays what is selected to delete.

Figure 5.4: Client Uninstall button



5. Click **Uninstall**. The system removes the application.
6. Click **Done**. The item is removed from the list of programs in the Control Panel.

Protex 7.8.6 and higher requires PostgreSQL version 13.3. As part of the Protex 7.8.6 upgrade, there are no additional steps required to upgrade to PostgreSQL 13.3 as it was all taken care of by ISO and Online update.

For additional information, refer to the PostgreSQL 13.3 documentation.

6.1 PostgreSQL Replication Slots

Replication Slots is a feature introduced in PostgreSQL 9.4 which allows the master and standby servers to better coordinate their state for additional reliability.

Enabling replication slots may be beneficial if it fits your workflow requirements. For more information, refer to PostgreSQL's `pg_replication_slots` documentation.

6.2 Database Settings with PostgreSQL

As of Protex versions 7.6 and higher, the `auto-conf.pgsql` file is internal to the installer and updates. Note that if Black Duck customer supports asks you to change a PostgreSQL setting, instead of editing the `postgresql.conf` file, make the required changes using the *alter system* commands for changing server configuration parameters. These commands are recorded automatically in the `postgresql.auto.conf` file. You can still make the required changes in `postgresql.conf`, but `postgresql.auto.conf` takes precedence.

Note: Changing certain parameters; for example, `shared_buffers`, still requires a database restart, regardless of how the parameter was changed. Changes to other parameters take effect the next time the database configuration is reloaded; either on receipt of a HUP signal, or in response to `pg_ctl reload`.

For additional information, refer to the PostgreSQL 13.3 Server Configuration documentation.

6.3 Database Backup with PostgreSQL

As of Protex version 7.6 and higher, PostgreSQL version 9.5.6 or higher is required. This version of PostgreSQL impacts the `pg_dump` command. The `pg_dump` command now includes the `--jobs` option, which reduces dump time by running multiple jobs in parallel, at the cost of a higher load on the server.

For more information, refer to the PostgreSQL 13.3 `pg_dump` documentation.

Appendix A: 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:

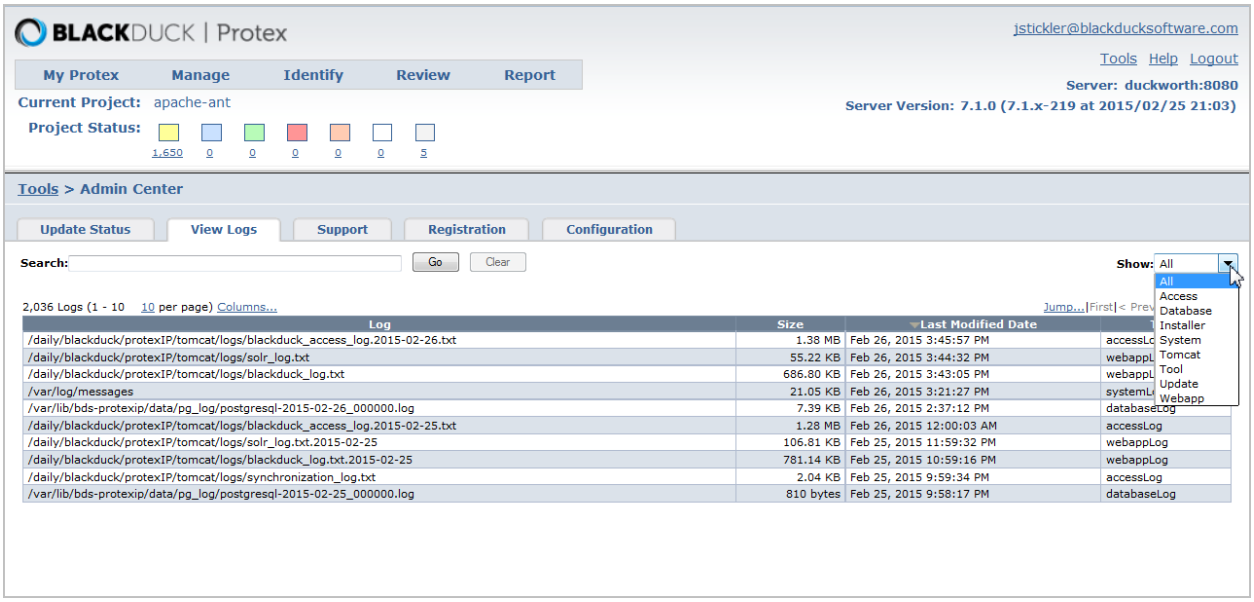
- **All** – Shows all log files available.
- **Access** – Lists all access logs.
- **Database** – Displays log files associated with the database in use.
- **Installer** – Displays all installation log files.
- **System** – Displays all system-related log files.
- **Tomcat** – Displays only Tomcat-related 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**.

A.1 Viewing Log Files

You can view log files from the Protex user interface.

Figure A.1: Tools > Admin Center > View Logs tab



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.

A.2 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 A.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>.`

Appendix B: Calculating Upgrade Requirements

This appendix provides a guideline for calculating disk space requirements for Protex updates.

The following information is provided as a guideline for estimating additional disk space required to install a KnowledgeBase update or Protex online update. Because the disk space requirements for updates are dependent on the size of customer databases, Black Duck Software cannot compute your disk space requirements in advance. However, using the following guidelines, you can perform these estimations.

The following formulas assume that you have followed the recommendations in this Installation Guide: each directory is installed in a separate partition, and each directory is entirely contained by that partition. In other words, the following process assumes that you have not used undocumented features like table spaces, did not move sub-directories or other partitions, or create symlinks.

Note: If you have used table spaces to spread the database over several partitions, Protex follows the symlinks when computing current size, and greatly over-estimates the space required in the top data directory.

Before downloading an update, Protex checks to ensure that you have enough disk space to download the update.

- To download an update, free space in the downloads directory equal to the size of the update is required, as displayed on the **Tools** > **Admin Center** > **Update Status** page. This initial check verifies that you have enough free space to store the complete download.

Before installing an update, Protex runs several checks to ensure that you have enough disk space to install an online update. If you do not have enough disk space, Protex logs a message in the `.install.log` file, and the text in the **Action** column in the Admin Center changes to **Download**.

- The first check is for 200% + 10KB of free disk space in the download directory. This is because for installing an update, you need twice the amount of free space in the downloads directory to extract the compressed file, plus 10 kilobytes.
- The second check is for enough free disk space to update your `bds-data` directory (raw fingerprint files). The space required to update the `bds-data` directory varies based on the number of update worker threads, which depends on the number of cores in your Protex implementation.
    - For 4 core systems, free disk space equal to 22% of the current size of the `bds-data` directory is required.
    - For 16 core systems, free disk space equal to 35% of the current size of the `bds-data` directory is required.
    - For 32 core systems, free disk space equal to 48% of the current size of the `bds-data`

directory is required.

The default location for this directory is `/var/lib/bds-protexip/bds-data`.

Note: This check is performed only for KnowledgeBase updates. Software updates do not require extra space in this directory.

- The third check is for free disk space equal to 20% of the size of the `PGDATA` directory free in its partition. Thus the space required for an update varies, depending on the current size of your database.
- The default location for the `PGDATA` directory is `/var/lib/bds-protexip/data`, but this location is customizable during installation. The actual location is set in the `bin/postgresql.sh` file (look for `PGDATA=` near the top of the file), and in `uninstall/instutil.properties` (search for `PROP_PGDATA=` in the file).
- The final check is for sufficient disk space in the `Solr` directory to allow for 20% growth in its size.

The default location for the `Solr` directory is `/var/lib/bds-protexip/solr`, but this location is customizable during installation.

Note: The Solr directory is new in Protex version 7.0. When you upgrade to Protex 7, the online update uses the default directory location.