CIS Installation and Upgrade Guide

Cisco Data Virtualization Suite

Version 7.0.5

First Published: November 21, 2014
Last Updated: February 17, 2017

Cisco Systems, Inc.

Preface

Obtaining Documentation and Submitting a Service Request

For information regarding anything within Cisco's Data Virtualization and Analytics product suite, including Cisco Data Preparation, please see:

https://supportforums.cisco.com/community/12298251/data-virtualization-software-cis

If you follow the page, you will automatically get email when new documents or comments are added. We look forward to seeing you on the site.

For general Cisco information, documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier font`	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Searching Across Multiple PDF Documents

When you are looking for information in the documentation set, you might want to search across multiple documents. You can use the free Adobe Reader to do this.

If the options described below are not available in your version of Adobe Reader, please update it.

To search your PDF documents

1. Open Adobe Reader.

2. From the File menu, choose Open. and open any PDF document.
3. From the Edit menu, choose Advanced Search.
4. Under Where would you like to search?, click All PDF Documents in.
5. Click My Documents and choose Browse for Location at the bottom of the drop-down list.
6. Browse to the location of all your PDF files.
7. Enter the search term and click Search.

   Acrobat lists all PDFs in the folder that contain the search string, and the number of occurrences in each.
8. Click the instance of the search term and its surrounding text to open the PDF to that page.

Document Change History

The table below provides the revision history for the *CIS Installation and Upgrade Guide*.

Version Number	Issue Date	Status	Reason for Change
7.0	November 2014		■ Major revision. ■ New installers. ■ New repository. ■ New data sources supported. ■ Adapter and Active Cluster install instructions incorporated in this manual.
7.0.1	March 2015		■ Supported information updates. ■ Corporate look and feel updates.
7.0.2	August 2015		■ Changed the title to more accurately reflect the contents. ■ Updated supported information and added descriptions for the default cache repository.
7.0.3	December 2015		■ Added information for the Advanced Data Source Adapters. ■ Updates supported information.
7.0.4	August 2016		■ Updates to supported information.
7.0.5	January 2017		■ Updates to supported information.

Installation Requirements and Support Information

This topic describes installation requirements and what CIS supports. It includes the following topics:

Disk Space and Physical Memory Requirements

CIS performance depends on processor speeds, available memory, network bandwidth, data source response times, query join types, the complexity of views, and many other implementation factors. Fast response times and support for a large active user base and large loads are achieved with:

- Fast multi-core CPUs
- Large amounts of RAM

- Ample disk space
- GB Ethernet network connections on the same subnet as the most heavily trafficked data source

If hardware configurations are less than optimal, CIS functions equally well, although more slowly, for most development tasks.

The following sections describe the minimum requirements for disk space and memory.

- Minimum Disk Space Requirements, page 6
- Physical Memory Requirements, page 6

Minimum Disk Space Requirements

CIS has these minimum disk space requirements:

- 500 MB for CIS installation
- 300 MB for the CIS repository database

Recommended disk space for CIS includes:

- 16 GB RAM
- 1 GB for cache
- 10 GB for a temp directory on the CIS installation partition

  By default, CIS creates a temp directory on the same partition on which it is installed. After installation, you can reconfigure the size and partition of the temp directory to accommodate large queries. For information about those configuration parameters, see the *CIS Administration Guide*.

- 1.2 GB of additional free space under the CIS Version Control System (VCS) directory is the required minimum for each user who uses the VCS.

  By default, CIS creates a VCS directory on the same partition on which it is installed.

  Different types of resources require different amounts of space to store. We recommend that you use 12KB per resource as a rough storage guideline. The following guidelines will help you figure out how to calculate your VCS directory storage needs.

  – If you have 100,000 resources, we recommend 1.2GB of space available for storing resources.

  – If you expect a large amount of check-ins to the VCS directory, we recommend that you allocate additional space in the VCS directory area which lives under the CIS installation (INSTALL_DIR\data\vcs).

  Typically, changes within version control systems are stored as textual diffs. Textual diffs can add up over time.

Physical Memory Requirements

CIS has these memory requirements:

- 200 MB for design and development
- 700 MB for deployment

These physical memory requirements are for running CIS and Studio. Further memory might be needed for running other applications.

To increase the performance of data processing with CIS, add more RAM. The only thing to consider when adding more RAM into your CIS environment is that when garbage collection processes are run they might take longer.

Port Requirements

By default, CIS Server listens to port 9401 for ODBC connections. The ODBC port number is always one greater than the server's web services HTTP base port which by default, is 9400. So the ODBC default port number is 9401. If SSL is used (encrypt is set to true), the ODBC driver automatically adds 2 to the port value so that the 9403 port is used. To determine the actual ODBC port settings, see CIS Port Settings for Client Connections to CIS.

Changing the HTTP base port value also changes the value of all derived ports after the next CIS restart (with the exception of the Repository and Cache database ports, which will remain the same).

Port number availability for CIS and Business Directory:

- CIS ports

CIS Ports Default	Description
9400	Web services HTTP port <— port needs to be exposed for non SSL CIS http access
9401	JDBC, ODBC, and ADO.NET <— port needs to be exposed for non SSL CIS client access
9402	Web services HTTP SSL <— port needs to be exposed for SSL CIS http access
9403	JDBC SSL, ODBC SSL, and ADO.NET SSL <— port needs to be exposed for SSL CIS client access
9404	Default caching database port
9405	[reserved]
9406	Monitor Daemon
9407	Active Cluster - JGroups (when installed)
9408	Repository
9409	Monitor (when installed)

- BD ports

Business Directory Ports Default	Description
9500	Web services HTTP port
9501	JDBC, ODBC, and ADO.NET
9502	Web services HTTP SSL
9503	JDBC SSL, ODBC SSL, and ADO.NET SSL
9504	[reserved]
9505	[reserved]
9506	Monitor Daemon
9507	[reserved]
9508	Repository
9509	Monitor (when installed)

Studio and Server Connectivity and Installer Limitations

You can sometimes mix versions of Studio and Server as follows within a major release.

Studio Version	Server Version	Support
older	newer	Active

Studio Version	Server Version	Support
newer	older	Not active

For example:

- Connecting a 7.0.0 Studio with a 7.2.1 or 7.2.2 Server is supported.
- Connecting a 7.2.1 Studio with a 7.2.0 Server is not supported.

Business Directory and Deployment Manager Limitations

You can sometimes mix versions of Business Directory, Deployment Manager, and CIS as follows.

BD/DM Web UI Version	CIS Version	Support
older	newer	Active
newer	older	Limited, Not active

For example:

- Business Directory 7.0.2 and 7.0.3 clients are not compatible with published resources from CIS 7.0.1.
- The use of Business Directory 7.0.3 clients with published resources from CIS 7.0.2 is supported.

Installer Limitations

- 64-bit installers are supported only on 64-bit platforms.
- Linux and Windows installers are available only on the x86 hardware platform..

Type of Client	Requirements
32-bit Studio client	■ They are at the same CIS version and patch level. ■ The Server version is newer than the Studio version and they are both within the same major CIS version.
64-bit Studio client	

CIS Supported Platforms

Studio can be installed and run on all Microsoft Windows platforms, but is not available for any UNIX platforms. Business Directory is supported on Windows and UNIX platforms only.

64-bit installers are provided for each of the Windows and UNIX platforms. In addition, separate JRE versions are provided for each platform (see JRE Support, page 8).

JRE Support

The JRE required for CIS for each platform is listed in the following table.

Platform	JRE Required
AIX	JRE 1.7.0 IBM AIX build pap3270_27sr1-20140411_01(SR1)
HPUX	1.7.0.09-jinteg_2014_02_03_13_09-b00

Platform	JRE Required
Linux	JRE 1.7.0_71-b14
Solaris	JRE 1.7.0_71-b14
Windows	JRE 1.7.0_71-b14

Operating System Support for Studio

Client-platform operating system support and patch levels are listed in the following table.

Operating System (Client)	Patch	CIS Support	Notes
Microsoft Windows 7		Active	x64 and x86
Microsoft Windows 8	SP1	Active	x64 and x86

There is a known limitation of Windows OS that can result in a UNC error when using CIS. The known issue is that:

- The Windows service process can't see any mapped network driver of a front end user session, because the Windows service is running under a different credential, and the mapped network driver is valid in the user session only.
- The Windows service process can see SYSTEM ODBC DSN only, any USER ODBC DSN is not visible to the Windows service.

To work around for this known issue, use the UNC path for CIS to access remote files.

Operating System Support for Server

Server-platform operating system support and patch levels are listed in the following table.

Operating System (Server)	Patch	CIS Support	Notes
AIX 6.1 (PowerPC)	6100-07 or higher	Active	64-bit versions are supported. CIS deploys in native 64-bit JVM on all supported 64-bit operating systems.
AIX 7.1 (PowerPC)	7100-01 or higher	Active	
Amazon Web Service (AWS) CentOS 7		Active	x64 Includes a Windows installer for Studio.
Amazon Web Service (AWS) Microsoft Windows 2012		Active	x64 Includes a Windows installer for Studio.
CentOS 5.10		Active	64-bit versions are supported. CIS deploys in native 64-bit JVM on all supported 64-bit operating systems. x64 and x86 architecture.
CentOS 6.5		Active	
Microsoft Windows Server 2008 R2 Enterprise	SP2	Active	CIS deploys in native 64-bit JVM on all supported 64-bit operating systems.
Microsoft Windows Server 2012 Standard		Active	x64.
Microsoft Windows Server 2012 R2 Standard		Active	
Oracle Linux 5.10 Red Hat compatibility mode		Active	x64.
Oracle Linux 6.5 Red Hat compatibility mode		Active	x64.
Red Hat Enterprise Linux v5.10	N/A	Compatible	64-bit versions are supported. CIS deploys in native 64-bit JVM on all supported 64-bit operating systems. x64.
Red Hat Enterprise Linux v6.6	N/A	Active	
Red Hat Enterprise Linux v7	N/A	Active	Red Hat provides a 64bit OS image for RHEL 7 that provides 64bit application support for CIS.
Solaris Sparc 5.10	N/A	Active	64-bit versions are supported. CIS deploys in native 64-bit JVM on all supported 64-bit operating systems.
Solaris 10 (SPARC)	N/A	Active	64-bit versions are supported. CIS deploys in native 64-bit JVM on all supported 64-bit operating systems.
SUSE Enterprise Linux v11.3	N/A	Active	
SUSE Enterprise Linux v12	N/A	Active	
Windows Server 2003 Datacenter Edition	N/A	Active	64-bit versions are supported. CIS deploys in native 64-bit JVM on all supported 64-bit operating systems.
Windows Server 2003 Web Edition	N/A	Active	

Driver Support

Driver	Server Version	CIS Support
ODBC	iODBC Driver Manager v3.521 for Linux	Active
ODBC	iODBC Driver Manager v3.521 for AIX (PowerPC)	Active
ODBC	iODBC Driver Manager v3.521 for HP-UX (PA-RISC, Itanium 32- and 64-bit)	Active
ODBC	iODBC Driver Manager v3.521 for Solaris (SPARC)	Active
ODBC	Windows Driver Manager	Active
JDBC	JRE v1.7 and conforms to JDBC API 4.0	Active
JDBC	JRE v1.6 and conforms to JDBC API 4.0	Active
ADO.NET	ADO.NET (32-bit and 64-bit)	Active

SNMP Support

The CIS system supports SNMP v1.

Web Service Protocols

Web Service Protocols	CIS Support
SOAP v1.1	Active
SOAP v1.2	Active
WSDL v1.1	Active
WSI-Basic Profile v1.0	Active
WSI-Basic Profile v1.1	Active
XPath v1.0	Inactive
XPath v2.0	Active
XQuery v1.0	Active
XSLT v1.1	Active
XSLT v2.0	Active

Directory Services Support for LDAP and Kerberos

The following LDAP directory services are compatible for the Cisco Information Server to use as a secure authentication service.

Directory Service	CIS Support	Notes
Active Directory 2008, 2012	Active	LDAP, LDAPS, Kerberos
Novell eDirectory 8.8 sp5	Active	

Directory Service	CIS Support	Notes
Oracle Directory Server Enterprise Edition 11.1	Active	LDAP, LDAPS

Options and Features Supported for Use with CIS

The Cisco Information Server product suite supports a large collection of data sources, connection protocols, features, and client interfaces that grows with each service pack and release. The following topics catalogs many of these items:

Web Browser Support

CIS web-based products runs on these Web browsers:

Web Browsers	CIS Support	Notes
Microsoft Internet Explorer	Active	Business Directory supports IE 10 or higher. When using IE 10, the Business Directory load time is slower than when using IE 11 or an alternative browser.
Mozilla Firefox	Active	
Chrome	Active	
Safari	Active	Not supported for web service API calls. Safari commonly has problems with websites requesting an SSL certificate, but not requiring one. Business Directory and Deployment Manager on Mac using a Safari browser, might experience this issue. Refer to topics provided by Apple support for how to work around this problem. You might need to delete certificates in your keychain and retype the product URLs to launch them properly.

Monitor requires a Web browser running Adobe Flash Player Version 10 or greater.

For the Monitor and Deployment Manager client web applications to function properly, the machine that is running a compatible browser must be running on a machine with Windows 7 or higher. For Windows 8, if you are using IE, then make sure all compatibility settings are enabled or specifically configure it for compatibility view for each of the CIS web based products. Occasionally the login screen for these web applications does not close automatically, you can close it and continue using the product or you can choose to run in a different browser.

For best results, when running Business Directory and Deployment Manager concurrently, use different browsers.

Online help (and long lists in Manager) might not display as expected in Chrome. You can switch to another browser to resolve the issue.

The CIS and Business Directory servers require a secure connection. So when you first connect a browser to any CIS web-based application, you might get a warning about connecting to an untrusted site.

Depending on your browser:

- You might be asked to allow the connection process to continue.
- You might want to configure it to trust the site so that warning messages no longer appear. For some site configurations this might require configuration of SSL connections for your entire CIS environment.

OAuth 2.0 Compatible Browsers

- OAuth 2.0 is compatible with the Chrome browser.

Directory Services Support for LDAP and Kerberos

The following LDAP directory services are compatible for the Cisco Information Server to use as a secure authentication service.

Directory Service	CIS Support	Notes
Active Directory 2008, 2012	Active	LDAP, LDAPS, Kerberos
Novell eDirectory 8.8 sp5	Active	
Oracle Directory Server Enterprise Edition 11.1	Active	LDAP, LDAPS

Driver and Protocol Support

CIS supports the following drivers for connections with CIS.

Driver	Server Version	CIS Support
ODBC	iODBC Driver Manager v3.521 for Linux	Active
ODBC	iODBC Driver Manager v3.521 for AIX (PowerPC)	Active
ODBC	iODBC Driver Manager v3.521 for HP-UX (PA-RISC, Itanium 32- and 64-bit)	Active
ODBC	iODBC Driver Manager v3.521 for Solaris (SPARC)	Active
ODBC	Windows Driver Manager	Active
JDBC	JRE v1.7 and conforms to JDBC API 4.0	Active
JDBC	JRE v1.6 and conforms to JDBC API 4.0	Active
ADO.NET	ADO.NET (32-bit and 64-bit)	Active

Supported Data Sources

CIS supports these data sources.

CIS supports OAuth 2.0 for HTTP-based data sources: SOAP, REST, WSDL, and XML-HTTP. It is also available for several Advanced Adapter data sources.

For other supported data sources and applications, see these sections:

- Supported Add-On Adapters, page 17
- Supported Advanced Data Source Adapters, page 18
- Supported Client Applications, page 22

Select Data Source Adapter field	CIS Support	Versions, Compatibility, and Notes
Apache Drill	Active	CAST AS functions are not supported.
Composite	Active	
Custom Java Procedure	Active	
DB2 V10.5 (Type4)	Active	
DB2 v9 (Type 2)	Active	
DB2 v9 (Type 4)	Active	Kerberos authentication is supported with DB2 V9 Type 4 adapter
DB2 z/OS (Type 4)	Active	
Data Direct Mainframe	Active	The Shadow RTE Server (version 6.1.4.7606 or later) must be installed on the DataDirect Mainframe computer and the Shadow RTE Client (version 6.1.1.1080 or later) must be installed locally on the computer hosting the CIS Server.
File (cache, delimited, and XML)	Active	For data sources that access a file share, the CIS service user account needs to have permission to read the file share.
Greenplum 3.3	Active	CIS capabilities with Greenplum have been developed and tested with a single node license.
Greenplum 4.1	Active	
Greenplum 4.3	Active	
HBase 0.98 (Apache Phoenix Driver)	Active	Introspection of HBase databases retrieves information from the system tables. User created tables are only introspected if they have been created using the Apache Phoenix shell. Requires installation of Apache Phoenix JDBC drivers, specifically those in phoenix-4.1.0-bin.tar.gz. For more information see the CIS Administration Guide.
HSQLDB 2.2.9	Active	
Hive 0.10 (HiveServer2)	Active	Cloudera CDH4. Kerberos is supported. For Hive data sources, CIS introspects tables and columns only.
Hive 0.12 (HiveServer2)	Active	For Hive data sources, CIS introspects tables and columns only.
Hive 0.13 (HiveServer2)	Active	Cloudera CDH5.3. Hortonworks HDP 2.1. Kerberos is supported. For Hive data sources, CIS introspects tables and columns only.
Hive 0.14 (HiveServer2)	Active	Cloudera CDH5.3. Hortonworks 2.2. Kerberos is supported. Trusted Delegation is not supported. For Hive data sources, CIS introspects tables and columns only.
Impala 1.0	Active	For Hive data sources, CIS introspects tables and columns only.

Select Data Source Adapter field	CIS Support	Versions, Compatibility, and Notes
Impala 2.0	Active	For Hive data sources, CIS introspects tables and columns only.
Informix 9.x	Active	
LDAP	Active	v3
Microsoft Access	Active	Windows platforms only
Microsoft Access (non-ODBC)	Active	Windows platforms only
Microsoft Excel	Active	2000
Microsoft Excel (non-ODBC)	Active	2000
Microsoft SQL Server 2008	Active	Kerberos authentication is supported.
Microsoft SQL Server 2012	Active	Kerberos authentication is supported with the 2008 driver.
Microsoft SQL Server 2014	Active	
MySQL 5.1	Active	
MySQL 5.5	Active	
Neoview 2.3	Active	
Neoview 2.4	Active	
Netezza 6.0	Active	NPS
Netezza 7.0	Active	NPS
OData	Active	Provides for some limited access to SharePoint data.
Oracle 11g (OCI Driver)	Active	11g R1, 11g R2, Oracle RAC Kerberos authentication is supported with thin driver version 11.2.0.4.
Oracle 11g (Thin Driver)	Active	11g R1, 11g R2, Oracle RAC Kerberos authentication is supported with thin driver version 11.2.0.4.
Oracle 12c (OCI Driver)	Active	Oracle RAC
Oracle 12c (Thin Driver)	Active	Oracle RAC
ParStream	Active	ParStream version 4.2.5.
PostgreSQL 9.0	Active	
PostgreSQL 9.1	Active	
REST	Active	Kerberos authentication is supported. NTLM authentication is supported.
RSS	Active	
Redshift	Active	The following trigonometric functions should not be pushed to Redshift data sources, because they might return incorrect results: SIN, COS, TAN, ASIN, ACOS, COT.
SOAP	Active	1.1, 1.2 Kerberos authentication is supported. NTLM authentication is supported.
SAP HANA SPS 09	Active	Support is for on premise SAP HANA deployments.
Sybase 12	Active	12.5 ASE

Select Data Source Adapter field	CIS Support	Versions, Compatibility, and Notes
Sybase 15	Active	15 and 15.5 ASE Kerberos authentication is supported.
Sybase IQ	Active	15
Sybase IQ (Type 2)	Active	15.2
Teradata 13	Active	13 and 13.10 Support for query band.
Teradata 14	Active	14.10 Might require installation of a Teradata 15 driver. Support for query band.
Teradata 15	Active	FastExport is not supported. The JDBC driver does not support CLOB columns with NULL values when using CIS to cache data into a Teradata 15 target. Support for query band.
Vertica 6.1	Active	
WSDL	Active	1.1 Kerberos authentication is supported. NTLM authentication is supported.
XML/HTTP	Active	Flat files or over HTTP. Kerberos authentication is supported. NTLM authentication is supported.

Supported Add-On Adapters

Consult your vendor specific documentation for detailed documentation of the objects and fields that have changed from version to version. These SAP adapters require the SAP JCo driver. Configuration steps can be found in Installing SAP JCo on Windows, page 56. OLAP Cube Support–With CIS 5.1.0.1 and later, you can create dimensional OLAP views in CIS.

CIS supports the following application data sources.

Adapter	Version Support
Active Cluster	
Oracle E-Business Suite Adapter	11.5.8, 11.5.10 and 12.1 on Oracle 9i and 10g
Salesforce.com Adapter	Version 37 You can install and use the Salesforce.com Adapter on all platforms that CIS supports. See Installation Requirements and Support Information, page 5.
SAP Adapter	5.0, 6.0, and above SAP R/3 v4.7

Adapter	Version Support
SAP BW Adapter	3.5 and 7.0
SAP BW BEx Adapter	3.5 and 7.0
Siebel Adapter	7.7, 7.8, 8.0

For installation and licensing instructions, consult Installing Optional CIS Products, page 49.

Supported Advanced Data Source Adapters

CIS supports the following application data sources.

Data Source Adapter	Versions, Compatibility, and Notes
Active Directory	LDAP v2 and v3 servers
Amazon DynamoDB	DynamoDB REST API Version 2012-08-10
Cassandra	Versions 2.1.7 and 3.0.0
Couchbase	Version 4.0 of the API
DynamicsCRM	Windows server 2012 R2, Windows Server 2012, windows server 2008 R2, Windows server 2008, and Windows Server 2003
DynamicsGP	Dynamics GP 2010, 2013, and 2015
DynamicsNAV	Dynamics NAV 2013, 2015, and 2016
Eloqua	Eloqua REST API and Bulk API version 2.0
Email	Standard IMAP client as specified in RFC 1730 and RFC 2060
Sharepoint Excel Services	Excel data from SharePoint 2013, 2016, and Online
Facebook	Facebook Graph API 2.0, 2.1, 2.2, 2.3
Google AdWords	API v201502 and v201601
Google Analytics	Google Analytics Management API v3.0, Google Analytics Core Reporting API v3.0
Google Apps	Google Contacts API v3.0, Google Calendar API v3.0, Google Drive Web API V2.0
Google BigQuery	Google BigQuery API v2.0
Google Sheets	Google Sheets API v3.0
HBase	
HubSpot	HubSpot REST API
JSON	Standard JSON format as specified in RFC 7519
Marketo	Marketo REST API v1, Marketo SOAP API v2.6
MongoDB	MongoDB 2.6 and 3.0
NetSuite	NetSuite SOAP APIs 2011-2015
OData	OData 2.0, 3.0, and 4.0
RSS	RSS 2.0 feeds
SharePoint	SharePoint Online, SharePoint 3.0, and SharePoint Server 2007, 2010, 2013
Twitter	Twitter REST API v1.1

Limitations:

- Sometimes, instead of returning an empty value, “Select * from table where columnname = 'value'” may throw an exception, if there is no value in the column.

- Some adapters support ORDER BY, but sometimes there are only a few objects within that data source that support ORDER BY. CIS displays a message if the tables do not support ORDER BY.
- Tables might need to be filtered with mandatory inputs for querying the contents for table scans to work as expected. For example for google apps directions, the starting location and ending location might be needed to retrieve the results.
- Sharepoint adapters support direct Kerberos authentication.
- Bulk inserts are not supported.
- GoogleSheets does not support client side filtering.
- Table names or column names with the period character are not supported.
- Eloqua data sources where the password value is entered when creating the data source will persist the password and it cannot be changed.
- For the Sharepoint Excel Services adapter, during introspection all String data types are mapped to VARCHAR.
- The DynamicsCRM, DynamicsNAV, DynanoDB, GoogleBigQuery, and SharePoint adapters do not support " is not null" syntax.
- Queries that contain " LIMIT" are not supported.
- For MongoDB, updating schema files within a running instance of CIS is not supported.
- Deployment Manager is case sensitive when using it with these adapters.
- Deployment Manager attributes for these adapters can cause plans to fail.
- “Ignore case sensitivity mismatch between CIS and data source” and “Ignore trailing space mismatch between CIS and data source” override the server side setting for a data source.
  By default these two overrides are enabled so that queries are always pushed. This is the case even when there is a mismatch and the query does not contain UPPER or RTRIM or similar options.
- Set these attributes to false or disable the push to get the consistent results as when the query is run with in the CIS.

For installation and licensing instructions, consult Installing Optional CIS Products, page 49.

For OAuth descriptions, see Configuring OAuth 2.0 for CIS Advanced Adapters, page 51.

Supported Cache Targets

CIS supports the following as cache targets:

Cache Target	CIS Support	Parallel Cache Target Support	Native Cache Target Support	Notes
File	Active	Active		
Greenplum 4.1	Active	Active	Active	
HSQLDB 2.2.9	Active	Active		
IBM DB2 LUW v9.5	Active	Active	Active	Native load with insert and select, and the DB2 LOAD utility are supported.
IBM DB2 LUW v10.5	Active	Active	Active	Native load with insert and select, and DB2 Load are supported.

Cache Target	CIS Support	Parallel Cache Target Support	Native Cache Target Support	Notes
Microsoft SQL Server 2008	Active	Active	Active	The DBO schema must be selected and introspected as a resource prior to attempting to cache data.
Microsoft SQL Server 2012	Active	Active	Active	The DBO schema must be selected and introspected as a resource prior to attempting to cache data.
Microsoft SQL Server 2014	Active	Active	Active	The DBO schema must be selected and introspected as a resource prior to attempting to cache data.
MySQL 5.1	Active	Active	Active	
MySQL 5.5	Active	Active	Active	
Netezza 6.0	Active	Active	Active	Native load with insert and select is supported. Parallel cache processing is achieved using the native DISTRIBUTE syntax. Procedure caching is supported.
Netezza 7.0	Active	Active	Active	Native load with insert and select is supported. Parallel cache processing is achieved using the native DISTRIBUTE syntax. Procedure caching is supported.
Oracle 10g	Supported			Native load with INSERT and SELECT is supported. Native load with DB link is not supported.
Oracle 11g and 11g R2	Active	Active	Active	
Oracle 12c	Active	Active	Active	
PostgreSQL 9.1	Active	Active	Active	Bulk load is supported. Native loading is supported when the source and target are the same database. If not then Parallel loading is used.
SAP HANA SPS 09	Active	Active		
Sybase ASE 12.5	Active			
Sybase ASE 15.5	Active			
Sybase IQ 15.2	Active		Active	
Teradata 13	Active		Active	Supported, but with limitations.
Teradata 13.10	Active		Active	Supported, but with limitations.

Cache Target	CIS Support	Parallel Cache Target Support	Native Cache Target Support	Notes
Teradata 14.10	Active		Active	Supported, but with limitations. Might require Teradata 15 driver.
Teradata 15	Active		Active	Choose tables For Caching is not supported.
Vertica 6.1	Active	Active	Active	Supports the use of native load and parallel cache load together. Native load with INSERT AND SELECT is supported.

Data Ship Source and Target Support

Data ship optimization is supported for following data source types.

Data Source Type	Data Ship Source Support	Data Ship Target Support	Performance Option	Notes
DB2 v10.5	Active	Active	Bulk Load using the LOAD utility	LUW
DB2 v9.5		Active		LUW
Microsoft SQL Server 2008	Active	Active	Bulk import/export using BCP	
Microsoft SQL Server 2012	Active	Active	Bulk import/export using BCP	
Microsoft SQL Server 2014	Active	Active	Bulk import/export using BCP	
Netezza 6.0	Active	Active	external tables	
Netezza 7.0	Active	Active	external tables	
Oracle 11g	Active	Active	Database Links	To use an Oracle data source for data ship, the DBA must install the DBMS_XPLAN package in the database and create an area for temporary tables. For this data source to participate in data ship, it must be specified as a data ship source. Participation as a data ship target is optional. If Oracle is both source and target, DB Link needs to be set up between the Oracle databases.
Oracle 12c	Active	Active	Database Links	
PostgreSQL	Active	Active	Database Links	

Data Source Type	Data Ship Source Support	Data Ship Target Support	Performance Option	Notes
Sybase IQ 15	Active	Active	Location: iAnywhere JDBC driver	For a Sybase IQ data source to participate in data ship, the QUERY_PLAN_TEXT_ACCESS database option must be set to ON. For this data source to participate in data ship, it must be specified as a data ship source. Participation as a data ship target is optional.
Teradata 13.00	Active	Active	FastLoad/ FastExport	For this data source to participate in data ship, it must be specified as a data ship source. Participation as a data ship target is optional. Teradata Fastload mode doesn't work correctly using the 14.10 JDBC driver when Teradata is the Target Data Source. To workaround this issue, use the Teradata JDBC 15 driver.
Teradata 13.10	Active	Active	FastLoad/ FastExport	
Teradata 14.10	Active	Active	FastLoad/ FastExport	
Teradata 15	Active	Active	FastLoad	
Vertica 5.0	Inactive	Inactive		
Vertica 6.1	Active	Active	Bulk load utility Export to another Vertica database	

CIS DDL Feature Support

CIS DDL (Data Definition Language) feature to CREATE and DROP tables directly in the following data sources:

- DB2
- MySQL
- Oracle
- SQL Server
- Netezza
- Teradata

Supported Client Applications

All other client applications are supported through the standard communication protocols that include JDBC and ODBC.

Client-Side Applications	CIS Support	Notes
Cognos 11 R3	Active	
Cognos v10.2.2 fixpack 5	Active	

Client-Side Applications	CIS Support	Notes
MicroStrategy 9.0.2	Active	CIS supports these data sources for use with MicroStrategy: Oracle 10g or 11g, Netezza 5 or 6, SQL Server 2008, and for mixed data coming from Oracle 11g and Netezza 6. Because MicroStrategy can create and delete data directly, you must have used Studio configured one of the following as a temporary tablespace to hold the created and deleted data: Oracle 10g and 11g, Netezza 5 and 6, SQL Server 2008, Teradata 13, MySQL 5, and DB2 v9.
MicroStrategy 9.2.1/9.2.1m on Windows I-Server	Active	
Tableau Desktop Professional Edition Version 7.0.13	Active	
TIBCO Spotfire	Active	

Client-Side Web Services

Client-Side Web Services	CIS Support
.NET Framework v1.1	Not Supported
.NET Framework v2.0	Active
.NET Framework v3.0	Compatible
.NET Framework v4.0	Active
.NET Framework v4.5	Active

Enterprise Service Buses

Enterprise Service Bus	CIS Support
Sonic 7.5	Active
TIBCO EMS 4.4	Active
OpenMQ 4.4	Active

Client-Side ADO.NET Driver Support

The CIS ADO.NET driver can be installed, uninstalled, or re-installed. It can support 32-bit and 64-bit Windows operation systems. CIS Software supports native ADO.NET driver functionality on the following Windows operating systems.

- Vista Business
- Vista Business x64
- Windows 7 Professional
- Windows 7 Professional x64
- Windows versions 2005, 2008, 2010, 2012 and 2013.

The CIS ADO.NET driver requires several things including:

- .NET Framework 2.0 to be installed on the host.
- Latest version of Windows XP, Windows Server 2003, Windows 7 Professional, or Windows Vista Business.

The Cisco Information Server (CIS) supports communication and use with:

- Visual Studio 2005 and 2008 edition Standard, Professional, or Team Developer versions
- Visual Studio 2010, 2012 and 2013

Data Sources Supported for Kerberos Token Pass-through

- IBM DB2 LUW versions 9 and 9.5 Type 4
- Oracle

  With these Kerberos authentication modes:

  - Microsoft memory-based
  - Ticket cache file-based
  - Specified data source name and password

  ...these Oracle data sources are supported for Kerberos:

  - Database version 11gR2 with an Oracle 11g driver
- Microsoft SQL Server 2008 and 2012
  - For Kerberos authentication, use the Microsoft SQL JDBC driver version 4.0.
- SOAP 1.1 and 1.2
- REST
- Sybase ASE v12 and v15
- WSDL 1.1
- XML over HTTP

CIS Operating Systems Support

- 64-bit Windows Server 2003, 2008, and 2010
- 64-bit RHEL AS 6.6 and 7.0

Communication Interfaces and Protocols

- ADO.NET
- JDBC
- OData
- ODBC
- Web Services

Security Features

Security features are discussed throughout this guide:

- SSL is available for silent mode installation (Silent Mode Installation, page 45) and for installing optional products (Installing Optional CIS Products, page 49).
- Kerberos can be used when connecting to several data sources (Supported Data Sources, page 14).
- Password protection is available for operations like installing and starting CIS and registering with data sources like SAP (Registering with the SAP System Landscape Directory, page 55).

Support and Maintenance Policies for Cisco Products

Cisco provides support and maintenance for major/minor releases of Cisco Information Server. For details of support and deprecation schedules, see the *CIS Release Notes*.

Support Policies for Third-Party Environments

All versions stated of an environment presume the initial release of a Third-party product without any need for patches, service packs or equivalent terms unless stated. Equally, unless stated, we presume that patches or service packs and minor version releases are upward compatible for our products. Whenever a new release of Cisco Information Server requires deployment of a patch or service pack or is compatible only with a minor version of an environment, Cisco will highlight these requirements in release notes and will require customers to install a patch or service pack or minor version to receive support and maintenance on the product.

The following classifications indicate the level of support for the current release.

Classification	Description
Active	All aspects (design/creation and runtime) are supported in Studio and Server.
Desupported Not Supported	Design/creation of platform version is no longer supported, runtime will persist until the next major or minor version. OR: This platform version has not been added to CIS yet.
Deprecated	Runtime removed from CIS. Old data sources will need to be upgraded to platform versions that are supported
Inactive	Design/creation and runtime are allowed in Studio and Server, no active testing or development of new features will be performed to the platform version

Support Policies for Third-Party Application Virtualization Environments

Customers deploying Cisco's products in third-party application virtualization environments from VMWare, Xen, and others should first consult the list of native host environments supported by the Cisco Information Server to verify compatibility. Support issues arising from deploying Cisco Information Server in any Third-party application virtualization environments will be reviewed and resolved only on the native host operating system to remove any incompatibilities that might be introduced by the application virtualization environment itself.

Limitations

Servlets are not supported and cannot be imported from previous versions of CIS.

Data Sources Not Supported by Discovery

Discovery supports all data sources and Cisco Adapters except the following:

Data Sources Not Supported by Discovery
Custom Java procedures—Not supported because they are procedural.
Hive
HP Neoview
IBM DB2 z/OS Version 8, Version 9, Version 10
Impala
Netezza
PostgreSQL
Relational data sources—Procedural objects in relational data sources are not supported.
SAP BW
SAP HANA
Teradata
Vertica
WSDL
XML (flat files or over HTTP)

Preparing for Installation

This topic focuses on preparations to install the Data Virtualization Platform, as follows:

Software Components for Installation

CIS provides the following installers for the Data Virtualization software components:

Installer	Included in the installer	
CIS Server	CIS Server Studio Deployment Manager Repository Java Monitor Discovery	Active Cluster Salesforce.com Adapter SAP Adapter SAPBW and BEx Adapters Oracle EBS Adapter Siebel Adapter Default cache database Advanced Data Sources Adapters
Studio	Studio	Java
Client	ODBC ADO.Net	Hadoop JDBC
Business Directory Server	BD Server BD Repository	BD web application Java

Some of these components need a separate license key to activate them.

About CIS Software Patches

CIS produces service pack patches as needed to update installed products. Patches are applied after the product has been installed. A patch is a zipped package of files that fixes known issues and which often provides enhanced functionality.

Install the most recent CIS patches on all computers running Server, Studio, and associated utilities. Specific patches might not be required for all CIS applications and services installed in a particular release. Typically, patches should be applied universally to avoid version mismatches.

You must use the Studio patch to get Studio client fixes.

For information about how to obtain and install the latest patch, see the *CIS and Business Directory Release Notes*.

Overview of Installation Steps

This section includes the following topics:

Installation Overview for New CIS Software Customers

If you are installing CIS Data Virtualization products for the first time, here is an overview of how you would proceed:

1. Review the new features and bug fixes as documented in the *CIS and Business Directory Release Notes*.
2. Review the information in the following topics:
   - Installation Requirements and Support Information, page 5
   - About CIS Software Patches, page 27
   - Preparing Your Systems for Installation, page 28
3. Install CIS as described in:
   - Installing Cisco Information Server, Studio, and Drivers, page 35
   - Silent Mode Installation, page 45
4. Apply the latest CIS Service Pack patch. Instructions for how to install a patch or service pack are subject to change with each service pack. For instructions, see the *CIS and Business Directory Release Notes*.

Installation Overview for Existing Customers Upgrading from a Previous Release

To install a major upgrade for CIS

1. Review the new features and bug fixes as documented in the *CIS and Business Directory Release Notes*.
2. Review the information in the following topics:
   - Installation Requirements and Support Information, page 5
   - About CIS Software Patches, page 27
   - Preparing Your Systems for Installation, page 28
3. Review and follow the steps in Upgrading from an Earlier CIS Release, page 31.
4. Backup all the data you want to save from the previous version of CIS.
5. Install the current version of CIS and any service packs.
6. Import the data from your previous version of CIS from the backup file.

Preparing Your Systems for Installation

To prepare your systems for installation

1. Review the new features and bug fixes as documented in the *CIS and Business Directory Release Notes*.

2. Review any README file included in your installation, patch, or service pack bundle.
3. Review the following requirements:
   - Installation Requirements and Support Information, page 5
   - You must have administrator privileges on the host computer to install Cisco Information Server.
   - You can have multiple JVMs running on the installation machine.
   - Server requires a block of nine ports for use by CIS and associated services. The port setting for Web services HTTP communication serves as the “base port”. By default, the base port is 9400, but you can change it after installation using configuration parameters.
4. Make sure that any LIBPATH or LD_LIBRARY_PATH environment variable that you might have does not begin with a " /" slash or end with a " :" colon. Those characters may keep the repository from starting successfully.
5. Review your firewall settings and verify that they allow access to the ports that CIS (Business Directory, Deployment Manager, and CIS) products need to use.
6. To see the current base port setting, choose Configuration from the Administration menu and navigate to Server > Web Services Interface > Communications > HTTP > Port (Current).

   Note: Changing the HTTP base port value also changes the value of all derived ports after the next CIS restart (with the exception of the Repository and Cache database ports, which will remain the same).

   These example ports are reserved or are derived from the base port:

```
9400 Web services HTTP port
9401 JDBC, ODBC, and ADO.NET
9402 Web services HTTP SSL
9403 JDBC SSL, ODBC SSL, and ADO.NET SSL
9404 Default caching database port
9405 [reserved]
9406 Monitor Daemon
9407 Active Cluster - JGroups (when installed)
9408 Repository
9409 Monitor (when installed)

9500 Business Directory
9502 Business Directory (reserved)
9508 Business Directory
```

7. Stop Server if an earlier version is running.
8. Shut down all other application programs running on the installation machine.
9. Make sure you know the hostname or the IP address of the installation machine.
10. If you are installing on a Linux operating system, see Preparing UNIX for CIS Installation, page 30.
11. If you are installing on a Windows operating system, see Preparing Microsoft Windows for CIS Installation, page 31.

Preparing UNIX for CIS Installation

This section applies only if you are installing CIS on a machine running a supported UNIX operating system. Examples of valid and invalid */etc/hosts* file entries are shown in the following table.

Validity	/etc/hosts File Entry
Valid	127.0.0.1 localhost IP hostname.domain hostname
Valid	127.0.0.1 localhost localhost.localdomain IP hostname.domain hostname
Valid	127.0.0.1 localhost localhost.localdomain localhost IP hostname.domain hostname
Invalid	127.0.0.1 localhost.localdomain IP hostname.domain hostname
Invalid	127.0.0.1 localhost.localdomain localhost IP hostname.domain hostname

To prepare your UNIX machine for installation of CIS products

1. Review the new features and bug fixes as documented in the *CIS and Business Directory Release Notes*.
2. Optionally for AIX, make sure that you have one of the following readline libraries installed:
   - readline-6.0-1.aix5.1.ppc.rpm
   - readline-6.0-3.aix5.1.ppc.rpm
   - readline-6.1-3.aix5.1.ppc.rpm
   - readline-6.2-5.aix5.1.ppc.rpm
   - readline-6.3-5.aix5.1.ppc.rpm
   - readline-6.1-1.aix6.1.ppc.rpm
   - readline-6.1-2.aix6.1.ppc.rpm
3. Run the following command to determine if localhost can be resolved on the target installation machine before attempting an installation:

   ```
   ping localhost
   ```

4. If the ping results look like the following, localhost is being resolved and the machine is ready for CIS installation. You can continue with the instructions in other sections.

   Linux Ping Example with Valid localhost

   ```
   $ ping localhost
   PING localhost (127.0.0.1) from 127.0.0.1 : 56(84) bytes of data.
   64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=255 time=0.071 ms
   64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=255 time=0.063 ms
   64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=255 time=0.043 ms
   --- localhost ping statistics ---
   3 packets transmitted, 3 received, 0% loss, time 1999ms
   rtt min/avg/max/mdev = 0.043/0.059/0.071/0.011 ms
   ```

5. If the ping results look like the following, localhost is not correct. You must edit your /etc/hosts file.

   Linux Ping Example with Invalid localhost

This example of /etc/hosts files shows where Server is unable to connect to the repository database because of the localhost.localdomain entry preceding the localhost entry (assuming the localhost entry exists at all).

```
$ ping localhost
PING localhost.localdomain (127.0.0.1) from 127.0.0.1 : 56(84) bytes of data.
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=1 ttl=255 time=0.080 ms
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=2 ttl=255 time=0.071 ms
64 bytes from localhost.localdomain (127.0.0.1): icmp_seq=3 ttl=255 time=0.044 ms
--- localhost.localdomain ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 1998ms
rtt min/avg/max/mdev = 0.044/0.065/0.080/0.015 ms
```

6. Edit the /etc/hosts file to add a localhost entry, directly after the 127.0.0.1 entry, with the following syntax:

```
127.0.0.1 localhost <optional host name>
```

7. Save your changes and rerun the ping for localhost.

Preparing Microsoft Windows for CIS Installation

If you are installing CIS on Microsoft Windows Vista Business Edition, Windows 2008, or Windows 7, you must disable User Account Control before installing Cisco Information Server.

To disable the User Account Control

1. From the Windows Start menu, select Control Panel > User Accounts > Change User Account Control Settings.
2. Change the setting to Never notify.

Upgrading from an Earlier CIS Release

This section is a guide for customers who are upgrading to CIS from a previous version and want to migrate metadata from that version to the new version.

Note: This process is different from many other software vendor upgrade procedures, which typically modify the existing instance.

The metadata upgrade process requires installing a new CIS instance in parallel with the existing CIS instance, exporting the metadata from the old instance, and importing the old instance's backup CAR file into the new CIS instance.

CIS recommends that you keep the older CIS instance until you are sure the new installation is stable. However, be aware that:

- If you are running two versions of CIS simultaneously, their port numbers must be different.
- If you are using Active Cluster, all servers in the cluster must be running at the same version and patch level.
- New instances of CIS can use the repository database of older instances.

Make sure that you have administrator privileges and perform all of the steps below as that user.

To upgrade and migrate your existing installation, follow the steps in these sections

1. Documenting the Existing CIS Instance, page 32
2. Considerations for Upgrading to CIS 7.0, page 32
3. Exporting Metadata from the Existing CIS Instance, page 32
4. Installing the New Version of CIS, page 33

5. Importing Metadata into the New CIS Instance, page 41
6. Verifying a Successful Installation, page 41

Documenting the Existing CIS Instance

Before making a backup of the existing CIS instance, document the key features of the instance. These settings are later applied to the new CIS instance to ensure the consistency of results returned from published resources.

Note: If you cannot upgrade directly from the existing CIS instance to the new version, multiple versions of CIS and multiple export and import processes might be required, so that database schemas remain compatible.

Make note of the settings in the following table.

Setting	What to Record
Ports	The port numbers for the existing instance, because after the installation of the new server is complete, the port numbers of the new instance might need to be changed.
Authentication mechanism	The authentication mechanism. If LDAP or another dynamic authentication is used, the same settings need to be applied to the new server. This setting determines various authentication mechanisms enabled within Server.
Users/groups	The groups created in Server and the users that belong to these groups. If LDAP authentication is used, note the LDAP groups that were imported into Server.
Metadata repository	The full path of the repository location and the administrator user ID and password.
Custom data sources	Custom data sources that were introspected and any custom drivers that were used to introspect these sources.
External libraries	Any external libraries that were referenced from the instance.
Customized settings, including JRE flags, managed and unmanaged memory	Configuration parameter settings for the existing Server instance. From the Administration menu, select Configuration and check all relevant parameter settings. The new CIS instance's settings should match the old instance settings if you want similar results and performance.

Considerations for Upgrading to CIS 7.0

CIS no longer supports external repository databases. With 7.0 use of the PostgreSQL database that is distributed with the CIS Server install is required.

Depending on what you might have previously been using as your repository database, you might want to keep a backup copy of that database if you suspect you might have a need to revert to a prior CIS install such as 6.2.6.

During the export you performed in Exporting Metadata from the Existing CIS Instance, page 32 all of the relevant information from your old repository was captured.

During the import you performed in Importing Metadata into the New CIS Instance, page 41 all of the relevant information from your old repository was transferred into the new CIS PostgreSQL repository database.

Exporting Metadata from the Existing CIS Instance

The first step for upgrade or migration is to export the existing metadata information from the repository. This process writes out a CAR file that includes six files containing metadata, scheduling, settings, and user information.

To run the export

1. Verify that you have administrator privileges.
2. Open a command prompt window.

3. Navigate to <CIS_install_dir>/bin.
4. Perform a full backup with the options that you need:
   - Using Studio. See “Using Studio for a Full Server Backup” in the *CIS User Guide*.
   - Using the CIS backup_export utility. For more information, see the *CIS Administration Guide*.
5. Locate and copy the resulting CAR file to a safe and easily accessible location for use later.

Installing the New Version of CIS

To install a new Cisco Information Server when you are upgrading from an earlier release

1. Review the new features and bug fixes as documented in the *CIS and Business Directory Release Notes*.
2. Install the new version of Server as described in Installing Cisco Information Server, Studio, and Drivers, page 35 or Silent Mode Installation, page 45.
3. Install the latest versions of all other CIS software that you use.
4. Set up any external libraries, including JDBC drivers, and then shut down and restart the server.
5. Deliver the upgraded drivers (the CIS ODBC driver and the CIS JDBC driver) to the dependent clients.
6. To ensure consistency in results and performance, make the configuration of the new server instance similar to the old instance.
7. Perform the instructions in Importing Metadata into the New CIS Instance, page 41.

Perform the instructions in Verifying a Successful Installation, page 41.

Tracking and Documenting Your Install or Upgrade

We recommend that you document the issues that you encounter during an upgrade and document all customizations made to your new CIS system, to help ensure that your next upgrade goes smoothly.

Installing Cisco Information Server, Studio, and Drivers

This topic describes how to install Cisco Information Server on both Windows and UNIX computers and then verify that the installation was successful.

Topics covered in this topic include:

Installing on Windows

This installation process is used to install one or more components of Cisco Information Server. You install CIS for Windows using the InstallAnywhere installer wizard.

Note: If you installed CIS on Microsoft Windows Vista Business Edition, Windows 2008, or Windows 7, see Preparing Microsoft Windows for CIS Installation, page 31.

Running the CIS Server Installer

This installer installs the following components:

- CIS Server
- Java
- Active Cluster
- SAPBW and BEx Adapters
- Studio
- Deployment Manager
- Monitor
- Salesforce.com Adapter
- Oracle EBS Adapter
- Default caching database
- Repository
- Discovery
- SAP Adapter
- Siebel Adapter
- Advanced Data Sources Adapters

To install CIS on a Windows computer

1. Read any README files included with or associated with the download file.
2. Run the installer executable for your platform.
3. Follow the prompts on the screen. Special characters and spaces are not supported for <CIS_install_dir>.

   You can select the defaults for the <CIS_install_dir> and the CIS Server base port number.

   You will be prompted for two different passwords.

CIS Password Type	Description
CIS Repository	This is the database that will be used to store all of the data and metadata about the items that you create within CIS. It also stored your configuration and other environment settings. Passwords with special characters that are supported by your operating system shell are fine to use.
Default Caching Database	This is the database that will be created for you to hold data that you want to cache using the default caching method. There are multiple caching options. You might want to note the password for future use of this database.

   The installation process might take a few minutes, during which progress windows are displayed.

4. Finish to exit the installer when the installation is completed.

   The Server starts automatically at the completion of the installation process. You can also start and stop the services as described in the *CIS Administration Guide*.

   Install and uninstall logs are called bitrock_installer_<number>.log while the installer is running. After installation is complete, the logs are named <product>_install or <product>_uninstall.log. The log files can be found in the following directories:

Platform	Default Location of Log Files
Unix	/tmp
Windows 2008, Windows 2012, Windows 7, Windows 8	C:\Users\<username>\AppData\Local\Temp
Windows 2003	C:\Documents and Settings\<username>\Local Settings\Temp\1

5. Optionally, download and install the latest CIS patch as described in *CIS and Business Directory Release Notes*.

Running the Studio Installer

This installer installs the following components:

- Studio
- Java

This installer can be run on each Windows machine that needs access to the CIS Server.

To install Studio on a Windows computer

1. Read any README files included with or associated with the download file.
2. Run the installer executable for Studio.
3. Follow the prompts on the screen.

4. When the installation is complete, click Finish to exit the installation program.

Studio automatically runs and prompts you for login information.

Installing the Drivers

This client distribution (driver zip) file includes the following components:

- ODBC
- ADO.NET
- Hadoop
- JDBC

This zip file can be unpacked on each machine that has client application that needs access to the CIS Server.

To install the drivers distributed with CIS

1. Read any README files included with or associated with the download file.
2. Locate and extract the drivers zip file.
3. Follow the instructions in the CIS Administration Guide for details on how to complete configuration of each driver.
4. When the installation is complete, click Done to exit the installation program.

Installing on UNIX

Your CIS Server can be installed on a UNIX machine. Studio is not available for UNIX and must be installed on a Windows machine. You can then connect the Studio client to the Server on the UNIX machine.

- Installing CIS Server on UNIX, page 37
- Installing Drivers on UNIX, page 39
- Setting the CIS Server to Start Automatically on UNIX, page 39
- Configuring Security Enhanced Linux Environments, page 40

Installing CIS Server on UNIX

This installer installs the following components:

- CIS Server
- Java
- Active Cluster
- SAPBW and BEx Adapters
- Default caching database
- Deployment Manager
- Monitor
- Salesforce.com Adapter
- Oracle EBS Adapter
- Advanced Data Source Adapters
- Repository
- Discovery
- SAP Adapter
- Siebel Adapter

To install CIS on a UNIX computer

1. Make sure you have reviewed and completed any necessary preparation as discussed in Installation Requirements and Support Information, page 5.

2. For CentOS, Red Hat Enterprise Linux, and Oracle Red Hat Enterprise Linux systems Security-Enhanced Linux (SELinux) must be disabled or in permissive mode. See Configuring Security Enhanced Linux Environments, page 40.
3. If necessary, log into the installation machine as a non-root user. Change your working directory to the user's home directory.
4. Run the following command for your platform:

   ```
   chmod 755 <installer file name>
   ```

5. Make sure that the directory and path that you expect to use for CIS does not contain any spaces.
6. Make sure that you have READ and WRITE permissions on the installation directory.
7. Run the following command to start the installation:

   ```
   ./<installer file name>
   ```

8. Follow the prompts on the screen. Special characters are not supported for <CIS_install_dir>.

   You can select the defaults for the <CIS_install_dir> and the CIS Server base port number. The value you use for <CIS_install_dir> cannot contain a space.

   You will be prompted for two different passwords...

Password Type	Description
CIS Repository	This is the database that will be used to store all of the data and metadata about the items that you create within CIS. It also stored your configuration and other environment settings. Passwords with special characters that are supported by your operating system shell are fine to use.
Default Caching Database	This is the database that will be created for you to hold data that you want to cache using the default caching method. There are multiple caching options. You might want to note the password for future use of this database.

9. Finish to exit the installer when the installation is completed.

   The Server starts automatically at the completion of the installation process. For information about automatically restarting CIS, see Setting the CIS Server to Start Automatically on UNIX, page 39. You can also start and stop Server as described in About the Installed CIS Services, page 41 and the *CIS Administration Guide*.

   Install and uninstall logs are called bitrock_installer_<number>.log while the installer is running. After installation is complete, the logs are named <product>_install or <product>_uninstall.log. The log files can be found in the following directories:

Platform	Default Location of Log Files
Unix	/tmp
Windows 2008, Windows 2012, Windows 7, Windows 8	C:\Users\<username>\AppData\Local\Temp
Windows 2003	C:\Documents and Settings\<username>\Local Settings\Temp\1

10. If installing CIS on AIX, make sure that MAX_MEMORY >1500MB is in the <CIS_install_dir>/conf/server/server.properties.

    The server.properties file is processed every time the server is restarted from `composite.sh monitor`.

11. Optionally, download and install the latest CIS patch as described in *CIS and Business Directory Release Notes*.

Installing Drivers on UNIX

These files contain the following driver components:

- ODBC
- ADO.NET
- Hadoop
- JDBC

To install the drivers

1. Make sure you have reviewed and completed any necessary preparation as discussed in Installation Requirements and Support Information, page 5.
2. If necessary, log into the installation machine as a non-root user. Change your working directory to the user's home directory.
3. Make sure that you have READ and WRITE permissions on the directory for which you want to unzip the contents of the file.
4. Locate and extract the drivers zip file.
5. Follow the instructions in the *CIS Administration Guide* for details on how to complete configuration of each driver.
6. When the installation is complete, click Done to exit the installation program.

Setting the CIS Server to Start Automatically on UNIX

If at any time after installing the software, you restart the UNIX installation machine, Server and the metadata repository do NOT start automatically (unlike when they start automatically after a successful installation of the software).

To configure the CIS service files cis.repository and cis.server

1. Log into the installation machine as root.
2. Change the working directory to <CIS_install_dir>/bin.
3. Run the following command as the root user:

   ```
   cis_install_services.sh
   ```

   This command prompts for a username, and other details to install and configure the service files cis.repository and cis.server.
4. Enter the name of the user to start CIS (not the root user) and the other information requested.

   The script then installs cis.repository and cis.server into an appropriate location on the installation machine and configures them. The location will be printed on your screen when the configuration is successful, so make note of this location, because you need this to perform verification of the service files.

   Note: Do not run the cis.repository or cis.server scripts in the <CIS_install_dir>/bin/ directory. These are template files used by cis_install_services.sh only and are not meant to be run.

   Running cis_install_services.sh does not interrupt any repository or server processes that are running, but prepares the machine for automatically starting those processes during restart of the UNIX-based computer.

To verify the CIS service files configuration

1. Go to the location noted previously from running cis_install_services.sh.

2. Enter these commands:

```
./cis.repository restart
./cis.server restart
./cis.cache restart
```

Now if the machine is rebooted, the monitor, server, and repository processes should automatically start once the machine is ready to go.

Configuring Security Enhanced Linux Environments

All UNIX instances that have SELinux = enabled need to be reconfigured to SELinux = permissive to allow connections to CIS and Business Directory. The SELinux configuration file is located under /etc/selinux/config.

To configure SE Linux environments

1. Run /usr/sbin/sestatus to validate the setting for SELinux. If the value is enabled, you must change it.
2. Login as root.
3. Edit your environment configuration file.
4. Change the value of SELinux to permissive (SELINUX=permissive).
5. Reboot.
6. Run /usr/sbin/sestatus to validate the setting for SELinux.

Installing on Amazon Web Service

The CIS Server is supported on Windows and UNIX. Studio requires a Windows-based OS to operate.

To install CIS on a Windows-based AWS

1. Install and configure a supported version of Windows for AWS.
2. Select and install the AIM for CIS.
3. Follow the install instructions in Running the CIS Server Installer, page 35.
4. Follow the install instructions in Running the Studio Installer, page 36.
5. Follow the instructions in the *CIS Administration Guide* to register you CIS licenses.

To install CIS Server on a UNIX-based AWS

1. Install and configure a supported version of Linux for AWS.
2. Select and install the AIM for CIS Server.
3. Follow the install instructions in Installing on UNIX, page 37.
4. Locate the CIS Studio installer that came bundled with your AIM.
5. Move the installer file to a Windows-based AWS or another Windows machine.
6. Follow the install instructions in Running the Studio Installer, page 36.
7. Connect to the CIS Server on your Linux AWS.
8. Follow the instructions in the *CIS Administration Guide* to register you CIS licenses.

Applying a CIS Patch or Service Pack

After installation of CIS, you might want to apply the latest CIS patch which might be a later version than what you just installed. It is recommended that you install a patch on all computers running CIS products to ensure complete compatibility and minimize unforeseen problems.

Note: Instructions for how to install a patch or service pack are subject to change with each service pack. For instructions, see the *CIS and Business Directory Release Notes*.

About the Installed CIS Services

The installation process installs the following services which are CIS processes that run in the background:

- server—the Cisco Information Server process.
- repository—the database repository used by Cisco Information Server.
- monitor—a process that monitors Cisco Information Server and ensures that it is always running.
- cache—a process that runs the default caching database.

All processes must be running for CIS to function properly.

For more information on configuring and starting CIS, see the *CIS Administration Guide*.

Importing Metadata into the New CIS Instance

If your are upgrading your version of CIS from an earlier version and you have completed the instructions in Exporting Metadata from the Existing CIS Instance, page 32, then follow the instructions in this section. If you are performing a new installation, you can skip these instructions.

After the new CIS instance is successfully installed, the metadata from old CIS instance needs to be imported into the new instance. After the import is successfully completed, settings such as JRE configurations, managed memory setting and ports can be updated on the new instance.

To run the import

1. Verify that you have administrator privileges.
2. Locate the CAR file that you produced from Exporting Metadata from the Existing CIS Instance, page 32.
3. Perform a full backup import with the options that you need:
   - Using the Studio Import dialog window. For more information, see the *CIS User Guide*.
   - Using the CIS backup_import utility. For more information, see the *CIS Administration Guide*.
4. Validate that the CIS resources or other settings are as you expect in the new version of Studio.

Verifying a Successful Installation

To verify that your installation of the CIS software was successful, follow the steps in this section.

To verify a successful installation

1. Start Studio. Follow instructions in the *CIS Getting Started Guide* or in the *CIS User Guide*.

2. If you have just completed an upgrade from one version of CIS to a new one, then we suggest that you complete these instructions:

   a. Determine a set of tests that will touch all published resources and all introspected data sources, and then apply the tests against:

   – The existing instance of CIS, as a sanity check.

   – The new instance of CIS, to ensure the same results are produced.

   b. Configure and use the PubTest tool to test all your published resources.

   The PubTest program can be configured to test all published resources using JDBC, ODBC, and Web services. Additional configuration might be required to test the ODBC and Web services. Starting with CIS 4.0, an end-to-end testing program referred to as PubTest (pubtest.java) is included with the CIS installation. This program is located in the <CIS_install_dir>\apps\jdbc directory. A PubTest.doc file in this directory provides additional documentation about using this tool.

Tips from an Expert if the Server Does Not Start

If the server does not start and the log files indicate that the cause is not enough heap memory, you can modify the default max memory setting.

The server.properties file is processed every time the server is restarted from `composite.sh monitor`.

To modify the max memory setting

1. Stop the server.
2. Increase the MAX_MEMORY value in the one of the following locations depending on your server:
   – <CIS_install_dir>/conf/server/server.properties
   – <BD_install_dir>/bd/conf/server/server.properties
3. If adjusting the heap size with MAX_MEMORY is not enough to allow large CAR files to load, you can try setting the following Studio configuration parameters back to their default values:
   – Default Bytes to Fetch—Default value is 100.
   – Default Rows to Fetch—Default value is 1000.
4. From the process manager for your platform, shut down and restart all CIS processes (such as the CIS Server and monitor).

Setting Up AES128 Password Encryption

When storing user passwords and passwords used in communications with data sources, CIS encrypts the passwords using standard encryption. We recommend that you set up CIS to use AES128 encryption for stored passwords to improve user and data security.

It is best to carry out this procedure before connecting data sources and adding users, so that CIS automatically encrypts passwords using AES128 for them. If you wait until after adding users, you need to change each user's password individually to have it be encrypted using AES128.

Note: The admin password is the most important one to have encrypted using AES128.

The server has encryption configuration parameters whose values you can set. We recommend that you set these values before creating the keystore file and restarting, so that no windows ever have invalid values.

There is no cluster sync of the keystore, nor sync via backup archive. The repository keystore belongs to the local installation only.

To set up AES128 password encryption

1. Select Administration > Configuration from the Studio menu.
2. Navigate to Server > Configuration > Repository Database > Encryption.
3. Specify a value for Keystore Password.
4. Open a command window.
5. Use an existing keystore file or to create a repository key, go to the conf/server/security directory and Invoke the following command:

   ```
   keytool -genseckey -alias repositoryKey -keyalg AES -keysize 128 -keystore
   <cis_repo_keystore.jceks> -storetype jceks -storepass <key-password-X> -keypass <key-password-X>
   ```

   CIS requires that both passwords in this command line be the same.
6. After the key has been generated, you can verify its presence using the following command:

   ```
   keytool -list -v -keystore <cis_repo_keystore.jceks> -storepass <key-password-X> -storetype jceks
   ```

   Where cis_repo_keystore.jceks is the name of your keystore file.
7. Restart the server.

Where to Go After Installation

For your next steps, particularly if you are new to CIS products, see the information in the following PDFs or on-line help. You can access the PDFs at <CIS_install_dir>/docs, or from within Studio at Help > Online Help.

Book Title	Description
Getting Started Guide	Contains a simple example to get you familiar with the Studio application.
Administration Guide	Contains procedures for: ■ Completing and configuring your CIS installation ■ Licensing CIS software ■ Starting and stopping CIS ■ Finding and interpreting log files ■ Setting up security ■ Setting up JDBC, ODBC, and other drivers
User Guide	Explains Studio features and how to create and publish resources
Client Interfaces Guide	Contains instructions, guidelines, and examples of how to access CIS resources through various client applications.

Silent Mode Installation

You can install in silent mode. A silent mode installation does not require any user input at the time of installation to complete the installation process. It does not have a graphical user interface (GUI) but instead uses the values from a response file to perform the installation.

Topics covered include:

Creating the Options File for a Silent Installation

Optionally, when running a silent mode installation you can use an options file that has specific key-value pairs.

To create the options file for a silent install

1. In a text editor, create a options file similar to the following:

Business Directory	`# Modify install directory and all port number references`
	`#`
	`mode=unattended`
	`install_directory=/opt/Cisco_Systems/BD_7.0`
	`server_port=9500`
	`repository_admin_password=password`
	`----------------------------------------`

CIS	`# Modify install directory and all port number references`
	`#`
	`mode=unattended`
	`install_directory=/opt/Cisco_Systems/CIS_7.0`
	`server_port=9400`
	`repository_admin_password=password`
	`database_admin_password=password`
	`----------------------------------------`

2. Edit the values within the file for your installation.

The following table describes the variables in the response file:

Variable	Description and Value

INSTALL_DIRECTORY	Directory in which to install the software referred to as <CIS_install_dir>.
	
	The value can be empty, or the directory can be non-existent. On UNIX, there can be no space in the directory name. Examples:
	
	`install_directory=/opt/Cisco_Systems/CIS_7.0`
	`install_directory=C:\Program Files\Cisco Systems\Studio 7.0`
	`install_directory=/opt/Cisco_Systems/BD_7.0`

REPOSITORY_ADMIN_PASSWORD	Password to access the repository database, which is automatically installed during the installation. PostgreSQL requires that the password you choose cannot contain a # or $.
SERVER_PORT	Defaults to 9400 for CIS and 9500 for Business Directory.
DATABASE_ADMIN_PASSWORD	The password used to access the default caching database, which is automatically created during installation. PostgreSQL requires that the password you choose cannot contain a # or $.

3. Save the file as <installer.properties>.

Running the Installer in Silent Mode

To run the installer in silent mode

1. Create the response file according to your system environment, and place it anywhere on the installation machine. See Creating the Options File for a Silent Installation, page 45.
2. Run one of the following commands:

Component	Command Options

CIS Server	■ command line options
	
	`<instFILE>.bin --mode "unattended" --install_directory "</opt/Cisco_Systems/CIS_7.0>" --server_port "9400" --repository_admin_password "password" --database_admin_password "password"`
	
	■ command line with option file
	
	`<instFILE>.bin --optionfile <OPTION_FILE>`

Studio	■ command line options
	
	`<instFILE>.bin --mode "unattended" --install_directory "/C:\Program Files\Cisco Systems\Studio 7.0"`
	
	■ command line with option file
	
	`<instFILE>.exe --optionfile <OPTION_FILE>`

Business Directory	■ command line options
	
	`<insFILE>.bin --mode "unattended" --install_directory "/opt/Cisco_Systems/BD_7.0" --server_port "9500" --repository_admin_password "password"`
	
	■ command line with option file
	
	`<instFILE>.exe --optionfile <OPTION_FILE>`

The variables are as follows:

- <instFILE> is the file name. For example, installCISv7000_win64.exe for a Windows CIS Server.
- <OPTION_FILE> is the name of the response file.

3. Verify that the installation was successful by looking for the CIS installation directory. You can also view success or failure messages in:
   - %HOMEDRIVE%\BD_install.log (Windows) or /tmp/BD_install.log (UNIX)
   - %HOMEDRIVE%\CIS_install.log (Windows) or /tmp/CIS_install.log (UNIX)
4. Optionally for CIS, complete the configuration in Configuring Security Enhanced Linux Environments, page 40.

Installing Optional CIS Products

This topic describes the installation of optional CIS products. These topics are covered in this topic:

Version Support

CIS supports the versions listed in Supported Add-On Adapters, page 17 and Supported Advanced Data Source Adapters, page 18.

Installation Requirements

Add-On Adapter Installation Requirements

Individual adapters have these requirements:

- SAP BW BEx Adapter should be installed on a separate machine from the SAP GUI, to avoid possible conflict between JCo versions. Installing the SAP Java Connector Library, page 55
- For Salesforce.com and SAP adapter installations, disable User Account Control.
- SAP BW can cause CIS errors similar to:

```
com.compositesw.cdms.webapi.WebapiException: Error [sapbw-2900000]: BAPI_ODSO_READ_DATA_UC failed:
Key figure 0CMPYPTAMT unknown in InfoProvider 0BP_REL
```

To avoid this error, locate and install the patch listed in SAP "Note 1243987 - Extraction from DataStore object fails." Install this patch, and use the program SAP_RSADMIN_MAINTAIN to set the parameter RSDRI_DS_NEW in the table RSADMIN to ' ' (empty or space).

Note: To upgrade from an earlier version of an adapter, install the new version and then see Importing Resources Defined in an Earlier Release, page 59.

Active Cluster Installation Requirements

This section lists the software and hardware requirements for Active Cluster. All data sources and databases that are supported with this release of CIS are supported by Active Cluster.

CIS File Customizations

The data source capability files and LDAP properties file are not automatically synchronized with other machines in the cluster. Therefore, if you customized the ldap.properties file or data source capability files on a CIS Server that will be in a cluster, you need to copy these files manually to all computers that are members of the cluster.

For example, if you modified the external domain configuration file and the data source capability file for DB2, you would need to copy the following files to all computers that are or will become members of the cluster:

```
<CIS_install_dir>/conf/server/ldap.properties
<CIS_install_dir>/apps/server/apps/dlm/cis_ds_db2/conf/db2.capabilities
```

Digital Certificates

A digital certificate ensures the identity of a particular computer and the data it transmits to another computer. Every server in an Active Cluster must have a digital certificate set up on the computer. A trial digital certificate is shipped with CIS Server but must be changed to ensure full security. See Updating the Digital Certificate to Secure Cluster Communication, page 59 for how to do this.

Supported Platforms

See Installation Requirements and Support Information, page 5 for a list of the platforms and protocols supported by Active Cluster.

Disk Space and Physical Memory

Active Cluster requires an additional 4 MB of disk space.

Load Balancer Requirements

Although a load balancer is not required to be used with Active Cluster, it is highly recommended to achieve the maximum benefits of using Active Cluster.

Licensing

The licensing type for all cluster members should be identical. See the *CIS Administration Guide* for more information about licensing.

Installing an Optional CIS Product

All optional CIS products are installed for you when you perform the CIS Server install. To activate them, register a valid license key for the products that you have purchased.

Licensing Your Additional CIS Products

Before you create or join a cluster, you must license Active Cluster on every computer that will become a member of a cluster. You should receive an Active Cluster license key through email from your CIS representative. This license key is required

Consider the following requirements:

- You must license every CIS computer that will be a member of a cluster.
- You cannot create a cluster with a mixture of trial license nodes and full license nodes; all members of the cluster must have the same license type.
- All cluster members must use the same level of encryption.

To license CIS products

1. See the *CIS Administration Guide*.

Configuring OAuth 2.0 for CIS Advanced Adapters

If your Advanced Data Source Adapters will make use of OAuth authentication, then there is extra configuration that you must perform. The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service for:

- A resource owner by authorizing the resource owner and the HTTP service
- A third-party application to manage authorization separately

This section includes:

OAuth Options Provided by CIS Advanced Adapters

CIS provides the following OAuth options:

Initiate OAuth field options	Description
GETANDREFRESH	Typically, this option can be established quickly by most users. The Get and Refresh option uses the client id and client secret to initiate the OAuth as described in the OAuth 2 RFC and requires interaction between client, resource owner, and the Authorization and Resource Servers. A browser must be launched to enable the granting of permissions. Required field: Client Id, Client Secret, OAuth Settings file Location

Initiate OAuth field options	Description
OFF	This configuration uses an OAuth Access Token to authorize to the back end; it doesn't initiate any OAuth flow. The OAuth access token needs to be provided as part of configuration. This method is recommended if the access token is already obtained using other means. Most OAuth providers have a way to generate access tokens, with the help of developer consoles or APIs. Access tokens do expire and it is your responsibility to provide a new access token, when the previous one expires. This makes it suitable for one time use or when the access tokens have long life. Required Field: OAuth Access Token
REFRESH	This option refreshes the access token using a refresh token, client id, and client secret, when the current access token is expired and the refresh is transparent to the user. It stores the new access token in the OAuth settings file. Typically, users do not need to enter anything. This option option is best where the Studio and the CIS Server cannot be run on the same machine. It does require that a refresh token be obtained out side of CIS using OAuth provider tools. Required fields: OAuth Refresh Token, Client Id, Client Secret, OAuth Settings file Location

Preparing Eloqua for OAuth Access through CIS

The Eloqua data source adapter does not permit the use of the loopback address "localhost" or "127.0.0.1" in the callback URL. To use Eloqua with CIS and OAuth, you must configure your system resolver to resolve the new hostname you choose for this purpose to the loopback address 127.0.0.1, and use that new hostname in the callback URL. You must also identify an unused port.

To prepare Eloqua for OAuth access

1. On your CIS Server host, add a new hosts file entry that maps the loopback address 127.0.0.1 to a fully qualified hostname not actually used on your network, such as "eloqualoopback.mycisserver.com."

   For example, on Windows add the following entry to your c:\windows\system32\drivers\etc\hosts file:

   ```
   127.0.0.1 eloqualoopback.mycisserver.com  # the fully qualified hostname for the Eloqua Callback URL
   ```

2. Choose an available port on the host running CIS for use in the Callback URL. For example: 12481.

3. Log into Eloqua and configure your app's AppCloud Developer Settings to reference that hostname and port in the Callback URL. For example:

   ```
   https://eloqualoopback.mycisserver.com:12481/
   ```

   The https protocol is required.

Configuring GETANDREFRESH OAuth access for Advanced Data Source Adapters

The GETANDREFRESH option is the most typical configuration method for configuring OAuth access for your CIS Advanced Data Source adapters.

To configure GETANDREFRESH OAuth access for Advanced Data Source Adapters

1. Start the CIS from the UNIX or Windows command line.

2. Start Studio on the machine where you are running the CIS Server.

3. Add a new data source for one of your Advanced Data Source Adapters.

4. Provide a unique name for your data source.

5. On the Basic tab, type your company name (or account identifier).
6. On the Advanced tab, enter values for the following fields:

Field	Description of Value
Initiate OAuth	Typically, et this to GETANDREFRESH. Or a refresh token can be obtained from the OAuth provider and provided along with the client id and client secret. Getting a Refresh token requires experience in using the developer APIs and console of the OAuth provider. Also, the token has to be obtained using the same client id and client secret that is configured in the data source.
OAuth Client Id App ID	Set this to the client Id (app Id) of your data source.
OAuth Client Secret App Secret	Set this to the client secret of your data source.
Other	Set this to the value of your data sources callback URL. For Eloqua, obtaining the callback URL requires some extra steps. `https://eloqualoopback.mycisserver.com:12481/`

After the initial authentication is run and the tokens have been obtained, they are written into the configured OAuth settings file.

7. Save your new data source.
8. From the Studio resource tree, open the data source that you just added, and select Test Connection. Or introspect the data source.

   The adapter opens the OAuth endpoint in your system default browser.
9. Using the browser, log in and grant CIS permission to the adapter application.

   For example, Eloqua calls your specified callback URL, appending the access token and other needed values, such as:

   ```
   https://eloqualoopback.mycisserver.com:12481/callback#access_token=2YotnFZFEjr1zCsicMWpAA&token_type=bearer&expires_in=86400&state=xyz
   ```

10. If or when the authentication certificates expire, you must perform this procedure again to allow CIS permission to the data in the data source.

Replicating your OAuth Configuration on Other Machines

After initial testing and development work with your Advanced Data Source Adapters within CIS and Studio, it is typical that authorization settings will need to be migrated or replicated on other machines within your CIS environment. You can do this using CAR files and by migrating the OAuth settings file.

Occasionally, your usage focus might also require the replication of the authorization settings. Some of these usage focuses include:

Usage Focus	Description
Importing/Exporting Archives and Deployment Manager	When the archive contains a data source configured for OAuth and when it is imported or migrated to the target server, the OAuth settings file is not automatically imported or migrated. OAuth settings file needs to be externally migrated or the OAuth flow has to be reinitiated in the target server.
Clustered Environment	In a cluster, data source configuration is synced across the members of the cluster. For OAuth providers, who allow multiple valid tokens, configure OAuth settings location to be same path. If that is not possible, provide a path on the shared file system, which is accessible to all the members. Shared file system path is needed in case, where the OAuth provider does not support multiple valid tokens.

To replicate your OAuth configuration on Other Machines

1. From the Studio resource tree open the data source for which you want to replicate OAuth configuration.
2. On the Advanced tab, locate and save the value of the following field:

OAuth Settings Location	The value of this field is the location where the adapter writes the authentication information. If working in a clustered environment, make sure this location is central to all the nodes of the cluster, or replicate the OAuth settings file to each cluster

3. Create a CAR file export of the data source for which you want to replicate OAuth configuration.
4. Copy the OAuth settings file and the CAR file to the new host machine.
5. Copy the settings file to the same directory location as was specified in the OAuth Settings Location for the data source that you are replicating.

   Doing this allows a data source imported from the source to be used in target without modifications.
6. Use Studio on the new host machine to import the CAR file of the data source you are migrating.
7. Test the connection of the data source. If necessary resolve any issues.

Installing the Siebel Data Bean JARs

For the Siebel adapter, you must install the Siebel Data Bean JARs to enable connectivity to Siebel. Because these JARs are present on the Siebel Server itself, you might need assistance from your Siebel System Administrator. Follow the process below.

To install Siebel Data Bean JARs

1. Create a directory for the Siebel Data Bean JARs in the following location; <version> is the Siebel version:

   <CIS_install_dir>/apps/dlm/app_ds_siebel/lib/<version>
2. Copy Siebel.jar and SiebelJI_enu.jar from directory below to the directory created in the previous step. <Siebel> is the root directory of your Siebel Server.

   <Siebel>/eaiconn/CLASSES

Registering with the SAP System Landscape Directory

After installing the Cisco software, you must register the installation with the SAP System Landscape Directory if you are using this feature. The procedures for both Windows and UNIX are shown below.

Registration Procedure for Windows

To register the installation with the SAP System Landscape Directory on Windows

1. Run the script sap_sld_register_util.bat under <CIS_install_dir>/bin with command-line arguments <SLDHost> <Port> <Username> <Password>.
2. If connecting through a proxy, modify the script line set JAVA_OPTS= to:

```
set JAVA_OPTS=-Dhttp.proxyHost=<server> -Dhttp.proxyPort=<port>
```

Registration Procedure for UNIX

To register the installation with the SAP System Landscape Directory on UNIX

1. Run the script sap_sld_register_util.sh under <CIS_install_dir>/bin with command-line arguments <SLDHost> <Port> <Username> <Password>.
2. If connecting through proxy, modify the script line JAVA_OPTS= to:

```
JAVA_OPTS=-Dhttp.proxyHost=<server> -Dhttp.proxyPort=<port>
```

Installing the SAP Java Connector Library

You must install the SAP Java Connector Library (SAP JCo), version 3.0.9, on the same computer as CIS. SAP JCo is available through the SAP Service Marketplace at www.service.sap.com. You need to be a registered customer to download from there. After you sign in, navigate to SAP Java Connector > Tools & Services and download the JCo distribution for the platform running CIS, then refer to the next section to validate the installation.

Note: In SAP JCo version 2.1.5, passwords are no longer automatically converted to uppercase when they are sent to SAP; instead, case is preserved, which could lead to log on failure. The easiest way to address this is to change the data source to use an uppercase version of passwords. See SAP Notes 817880 and 792850 for more information.

It is best not to install the SAP Adapter on the same machine as the SAP GUI, to avoid a possible conflict between JCo versions.

SAP JCo and Large Volumes of Data

JCo has known memory limitations when processing queries. Severe cases can affect the main CIS Java process. In such cases, we recommend that large queries be divided into small queries.

Installing SAP JCo on Windows

You need to obtain the SAP Java Connector for your machine from SAP. Cisco has tested version 3.0.9 of the SAP Java Connector.

To install SAP JCo on Windows

1. Unzip the SAP JCo zip file into a temporary directory.
2. Copy sapjco3.jar to <CIS_install_dir>\jre\lib\ext.
3. Copy sapjco3.dll to one of these directories:
   - For Windows 32: <CIS_install_dir>\apps\common\lib
   - For Windows 64: <CIS_install_dir>\apps\common\lib\win64
4. Add a system PATH variable to point to the directory where you put your library files in the previous step.
5. Verify that the Windows system directory includes the files MSVCR71.DLL and MSVCP71.DLL.

   These DLLs are the Shared C Runtime (CRT) Components required by SAP JCo but are not shipped with it. If these DLLs are missing, install the Microsoft .NET Framework SDK Version 1.1. Microsoft .NET Framework SDK is available from the Microsoft Developer Network (MSDN) download site.

Testing the SAP JCo Installation on Windows

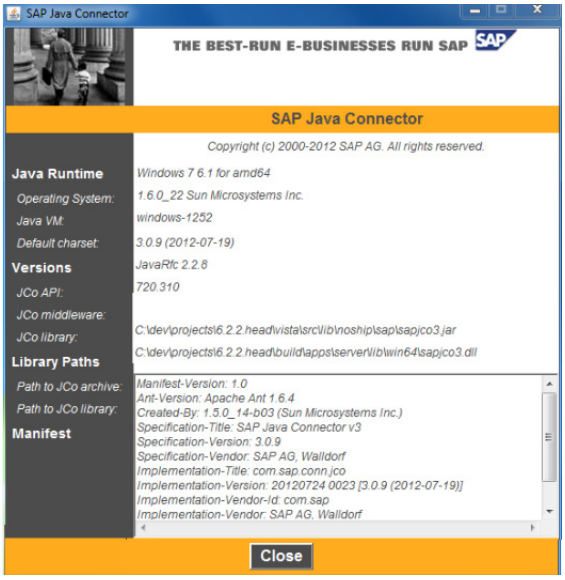
Be sure to test that the SAP JCo installation works correctly before using CIS.

To test the installation of SAP JCo on Windows

1. Ru**n the sapjco3.jar Java** executable using one of these commands:

Platform	Command
32-bit	`<CIS_install_dir>\jre\bin\java -Djava.library.path="<CIS_install_dir>\apps\common\lib" -jar "<CIS_install_dir>\jre\lib\ext\sapjco3.jar"`
64-bit	`<CIS_install_dir>/jre/bin/java -Djava.library.path="<CIS_install_dir>\apps\common\lib\win64" -jar "<CIS_install_dir>\jre\lib\ext\sapjco3.jar"`

2. Verify that running sapjco3.jar results in a screen that looks like this.



If an error message appears instead, SAP JCo needs to be re-installed.

Installing SAP JCo on UNIX

Follow the instructions to install SAP JCo based on the type of UNIX system you have. You need to obtain the SAP Java Connector for your machine from SAP. Cisco has tested versions of the SAP Java Connectors up to 3.0.9.

To install SAP JCo (Linux, Solaris, and AIX):

1. Unzip the SAP JCo tgz file for your machine into a temporary directory.
2. Copy sapjco3.jar to <CIS_install_dir>/jre/lib/ext directory, where <CIS_install_dir> is the root directory of your Cisco Server.
3. Copy libsapjco3.so into one of these directories:
   - Linux 32: <CIS_install_dir>/jre/lib/i386
   - Linux 64: <CIS_install_dir>/jre/lib/amd64
   - Solaris 64: <CIS_install_dir>/jre/lib/sparcv9
   - AIX 64: <CIS_install_dir>/jre/lib/ppc64
4. (For Linux and Solaris) Add a system LD_LIBRARY_PATH variable to point to the directory where you put your library files in the previous step.
5. (For AIX) Add a system LIBPATH variable to point to the directory where you put your library files in the previous step.

To install SAP JCo (HP-UX):

1. Unzip the SAP JCo tgz file for your machine into a temporary directory.
2. Copy sapjco3.jar to <CIS_install_dir>/jre/lib/ext directory, where <CIS_install_dir> is the root directory of your Cisco Server.
3. Copy libsapjco3.sl into this directory:
   - HP-UX 64: <CIS_install_dir>/jre/lib/PA_RISC2.0W

4. Add a system SHLIB_PATH variable to point to the directory where you put your library files in the previous step.

Testing the SAP JCo Installation on UNIX

It is critical to verify that SAP JCo is working before you attempt to connect to SAP using CIS.

To test the UNIX installation

1. From the command line, run the following command:

   <CIS_install_dir>/jre/bin/java -Djava.library.path=/<LIBRARY_PATH> -jar <CIS_install_dir>/jre/lib/ext/sapjco3.jar -stdout

   Where LIBRARY_PATH is the path for your system:

   - Linux and Solaris: $LD_LIBRARY_PATH
   - AIX: $SHLIB_PATH
   - HPUX: $LIBPATH

2. Verify that your output resembles the text below. If this command runs without error and the JCo API, middleware, and libraries have version information listed, then SAP JCo is properly installed.

```
---------------------------------------------------------------------
|                              SAP Java Connector                   |
|          Copyright (c) 2000-2012 SAP AG. All rights reserved.     |
|                             Version Information                   |
---------------------------------------------------------------------
Java Runtime:
 Operating System:       AIX 5.3 for ppc64
 Java VM:                1.6.0 IBM Corporation
 Default charset:        ISO-8859-1
Versions:
 JCo API:                3.0.9 (2012-07-19)
 JCo middleware:         JavaRfc 2.2.8
 JCo library:            720.310
Library Paths:
 Path to JCo archive:    /opt/Cisco_Systems/CIS_7.0.0/jre/lib/ext/sapjco3.jar
 Path to JCo library:    System-defined path to libsapjco3.a
---------------------------------------------------------------------
|                                  Manifest                         |
---------------------------------------------------------------------
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.6.4
Created-By: 1.5.0_14-b03 (Sun Microsystems Inc.)
Specification-Title: SAP Java Connector v3
Specification-Version: 3.0.9
Specification-Vendor: SAP AG, Walldorf
Implementation-Title: com.sap.conn.jco
Implementation-Version: 20120724 0023 [3.0.9 (2012-07-19)]
Implementation-Vendor-Id: com.sap
Implementation-Vendor: SAP AG, Walldorf
Main-Class: com.sap.conn.jco.rt.About
---------------------------------------------------------------------
```

Verifying a Successful Activation of an Adapter

Verification ensures that the adapter (which includes Advanced Data Source Adapters) was successfully installed and available as a data source.

To verify a successful activation

1. Start and log into Studio.
2. In the resource tree on the left, select a location to add a data source, right-click, and select New Data Source.

   In the New Physical Data Source window that opens, your adapter should appear in the list of data source drivers, indicating a successful installation.
3. Click Cancel.

Importing Resources Defined in an Earlier Release

If you used a previous release of the adapter and defined resources, you can use them with this release. Follow the instructions for exporting and importing the resources in the *CIS User Guide*.

Manage Active Cluster Security

Users who create and manage an Active Cluster must have administrative privileges. SSL is used for inter-node communications and each server in an Active Cluster must have a valid digital certificate for authentication.

All cluster members must use the same level of encryption.

- Updating the Digital Certificate to Secure Cluster Communication, page 59
- Set Access Privileges, page 59

Updating the Digital Certificate to Secure Cluster Communication

Every CIS Server ships with a trial digital certificate so SSL works right out of the box. However, the security is poor. To secure cluster communication, you must update the digital certificate on each CIS Server node in the cluster.

Updating the digital certificate entails getting a signed digital certificate from a Certificate Authority (CA) and installing it in the keystore on each CIS Server. CAs are independent vendors (such as VeriSign) that have instructions on their websites for how to generate public key/private key pairs that accompany certificate requests. The CA then returns the digital certificate back to you. After you have this information, you need to install the digital certificate on the CIS Server.

To install a digital certificate on CIS Server

1. Open Studio, and select Administration > Launch Manager (Web) from the menu to open the Manager Web interface.
2. Click the CONFIGURATION tab and select SSL.

   Manager displays the SSL Management page.
3. Enter new values as appropriate for your digital certificate, and click APPLY.

Set Access Privileges

You must have administrative privileges for Active Cluster management. Refer to the *Active Cluster Guide* for the specific rights needed for various cluster operations. Refer to the *Administration Guide* for more information about setting CIS access rights.

Uninstalling CIS

This topic describes the process of uninstalling Cisco Information Server (CIS) and related products for Windows and UNIX. The uninstall process is similar, regardless of whether you performed a silent or interactive installation.

Uninstalling CIS on Windows

When you uninstall CIS, everything stored in the metadata repository is deleted along with the CIS software.

To uninstall CIS on Windows

1. Stop the Server and Repository if they are running.
2. Start the uninstallation process:

   ... > Uninstall CIS

   For a silent uninstall, CIS is uninstalled without further interaction. For an interactive uninstall, go to step 3.
3. Click OK to confirm the uninstall.
4. Click Done when the uninstallation process is completed.

Uninstalling CIS on UNIX

The following tasks are described here:

Preparing for Uninstalling on UNIX

Before you uninstall CIS, remove the CIS service files from the installation machine, because the uninstaller does not remove these files automatically.

To remove the CIS service files cis.repository and cis.server

1. Log into the installation machine as root.
2. Change the working directory to <CIS_install_dir>/bin.
3. Run the following command:

   ```
   cis_remove_services.sh
   ```

Uninstalling CIS On UNIX

During the uninstallation process, all the components from the previous installation are removed. You cannot uninstall the components individually.

Note: On an HP machine, the uninstaller does NOT delete the <CIS_install_dir>, because the Java process under <CIS_install_dir>/jre has the directory locked.

To uninstall CIS on UNIX

1. Log into the installation machine as the user that installed the software.
2. Run the following command:

   ```
   <CIS_install_dir>/uninstall
   ```

   For a silent uninstall, run

   ```
   ./uninstall --mode "unattended"
   ```

   For an interactive uninstall, go to step 3.
3. Press the Enter key.

   You will see a warning about loss of data.
4. Press the Enter key to complete the uninstallation process and leave the uninstaller.