TIBCO® Data Virtualization

Security Features Guide

Version 8.1

Last Updated: *March 8, 2019*

Two-Second Advantage®

Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER

PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENTATION IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE "LICENSE" FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENTATION IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document contains confidential information that is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIBCO and the TIBCO logo are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries

TIBCO, Two-Second Advantage, TIBCO Spotfire, TIBCO ActiveSpaces, TIBCO Spotfire Developer, TIBCO EMS, TIBCO Spotfire Automation Services, TIBCO Enterprise Runtime for R, TIBCO Spotfire Server, TIBCO Spotfire Web Player, TIBCO Spotfire Statistics Services, S-PLUS, and TIBCO Spotfire S+ are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. SEE THE README FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENTATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENTATION. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENTATION AT ANY TIME.

THE CONTENTS OF THIS DOCUMENTATION MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

Copyright © 2004-2019 TIBCO Software Inc. ALL RIGHTS RESERVED.

TIBCO Software Inc. Confidential Information

Contents

Preface

Documentation for this and other TIBCO products is available on the TIBCO Documentation site. This site is updated more frequently than any documentation that might be included with the product. To ensure that you are accessing the latest available help topics, please visit:

- https://docs.tibco.com

Product-Specific Documentation

The following documents form the TIBCO® Data Virtualization(TDV) documentation set:

- *TIBCO TDV and Business Directory Release Notes* Read the release notes for a list of new and changed features. This document also contains lists of known issues and closed issues for this release.
- TDV Installation and Upgrade Guide
- TDV Administration Guide
- TDV Reference Guide
- TDV User Guide
- TDV Security Features Guide
- TDV Business Directory Guide
- TDV Application Programming Interface Guide
- TDV Tutorial Guide
- TDV Extensibility Guide
- TDV Getting Started Guide
- TDV Client Interfaces Guide
- TDV Adapter Guide
- TDV Discovery Guide
- TDV Active Cluster Guide
- TDV Monitor Guide
- TDV Northbay Example

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website mainly in the HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

Documentation for TIBCO Data Virtualization is available on https://docs.tibco.com/products/tibco-data-virtualization-server.

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit https://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, you can request one by clicking **Register** on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to https://community.tibco.com.

About TDV and BD Security Features

The TIBCO® Data Virtualization (TDV) and Business Directory (BD) have many security features and design considerations engineered to work together as an integrated system. These features keep information secure and available for use by only authenticated and authorized individuals with the appropriate rights and privileges.

Because TDV and BD are installed together and work in concert, references to TDV security apply to BD as well.

- TDV installer security during silent and interactive installations
- Security domains
- Internal repository security
- Log file security
- Encryption
- Export files security
- Cached data security
- Monitor security
- JDBC, ODBC, and ADO.NET TDV client security
- Manager client security
- Studio client security
- Web service client security
- Web service security standards
- Legacy web service security standards (transport layer and data source security)
- Security for the "composite" domain

For a discussion of user rights and privileges, refer to the *TDV Administration Guide*.

Note: This document lists the supported security features, but does not describe them in detail or explain how to set them up. Details and setup instructions can be found in other TDV and BD manuals. Each manual that contains security information has a centralized cross-reference list in its introductory chapter.

Security Feature Highlights

The following are the highlights of TDV security features:

- Passwords sent by JDBC and ODBC to TDV are encrypted.
- Passwords passed between TDV components are encrypted.
- Passwords in HTTP/SOAP headers for administrative functions are encrypted.
- All communication between TDV and Studio can be encrypted using SSL/HTTPS. Note: Older TDV and Business Directory were configured to use only TLSv1 by default. If you want to explicitly set the TLS version then please refer to the "SSL Protocol Configuration" section. Otherwise, the default TLS version will default to highest supported version that is negotiated between TDV and Studio (i.e. JRE 1.8 defaults to TLS v1.2).
- WSS Web service client security is supported.
- TDV to data source SSL is supported with or without Web Service client authentication where permitted.
- Passwords in metadata are encrypted.
- Passwords for LDAP and dynamic domain users are encrypted or not stored.
- Support for case-sensitive user login for external LDAP is supported.
- Options to include or exclude encrypted user passwords, repository passwords, LDAP, and data source passwords in export files.
- DBA password for the repository is not stored.
- Repository password and the repository connection with TDV are encrypted.
- Passwords are not shown in the log files.

For information on how administrators can delegate administrator rights, add LDAP users to a TDV group, and grant/revoke access privileges on TDV resources, see the *TDV Administration Guide.*

TDV Security Features by Component

The TIBCO® Data Virtualization (TDV) forms the core of the Data Virtualization Platform. You can use this document to evaluate TDV security features.

Topics covered in this chapter:

TDV Installer Security

TDV supports security for both silent and interactive installation.

TDV installers running in the UI or console mode do not store clear text passwords in any log files. The database administrator password for the repository is not stored.

The TDV installer installs a PostgreSQL database.

Security During Interactive or Silent Installations of TDV

TDV only creates the following messages about passwords in log files from the generation of the keystore file for the TDV Repository.

```
Initialization underway...

[04:30:37] Generating a keystore file for repository.
Executing /data/dev/<TDV_install_dir>/jre/bin/keytool -genseckey -alias repositoryKey -keyalg AES -keysize 128
-keystore cis_repo_keystore.jceks -storetype jceks -storepass **** -keypass ****
Script exit code: 0

Script output:


Script stderr:


[04:30:37] Verifying generation of a keystore file for the repository.
Executing /data/dev/<TDV_install_dir>/jre/bin/keytool -list -v -keystore cis_repo_keystore.jceks -storepass ****
-storetype jceks
Script exit code: 0
```

Configuring Security Enhanced Linux Environments

All Redhat OS Linux variants that have SELinux support can utilize it enabled (i.e. SELinux = enabled). If one wants to run TDV and/or Business Directory with SELinux enabled then an appropriate security policy that allows read/write access to the TDV installation directory and TDV ports is required before installation.

SELinux configuration file is located under /etc/selinux/config.

To configure SE Linux environments

1. Login as root on your Linux instance.

2. Run /usr/sbin/sestatus to validate your setting for SELinux.

3. If SELinux=enabled then you will need to make sure the following is part of your security policy.

a. TDV installation directory (TDV and/or Business Directory) must have read and write privileges on that directory and all files/directories underneath.

b. TDV ports (refer to Installation Guide "Port Requirements" section regarding what ports to allow)

Script output:Repository Security

This section describes TDV security for its repository when it is an internal implementation.

The password for the repository connection is encrypted.

For a brief time after initial installation, the repository connection password is in clear text. The first time TDV starts after initial installation, if it detects that the repository connection password is in clear text, it encrypts the password and stores it as a file name and key.

- File name: <TDV_install_dir>/conf/server/server_values.xml
- Key: /server/config/database/databasePassword

Administrator passwords for LDAP domains are encrypted. The database admin password appears in cis.repository while the installer_services.sh script is running. When the script is completed, the password is automatically deleted from cis.repository.

Repository and Cache Database Access and Privileges

The installer creates the repository and cache databases, it sets access and privileges for root, cisrepo and tutorial users.

The root user account is the DBA account for the entire PostgreSQL database.

The cisrepo user account is used to manage the TDV Server repository and cache databases.

The tutorial user account is used to manage the example Postgresql database used by the TDV Server for demo purposes.

Remote Access to the Repository

No user can access the repository nor the cache database remotely.

It is configured to only allow local connections.

Repository Settings

Repository settings are as shown in the following table.

Repository DB Name	Owner	Access privileges
cisrepo	cisrepo	cisrepo=CTc/cisrepo
inventory	tutorial	tutorial=CTc/tutorial
orders	tutorial	tutorial=CTc/tutorial
postgres	root	
template0	root	=c/root + root=CTc/root
template1	root	=c/root + root=CTc/root

Cache Settings

Cache database settings are as shown in the table.

Cache DB Name	Owner	Access privileges	
ciscache	ciscache	ciscache=CTc/ciscache	
postgres	root		
template0	root	=c/root	+ root=CTc/root
template1	root	=c/root	+ root=CTc/root

Data cached to relational databases is stored in clear text.

If flat file caching is used, the data is saved in binary format on the TDV installation drive and rendered in clear text. Secure access to HOMEDRIVE/temp or the customized location can be configured for file caching.

Log File Security

Passwords that occur in log files generated by TDV and clients are obfuscated.

Encryption

This section describes TDV password encryption.

TDV uses AES and Tiny Encryption Algorithm Variant (TEAV) for password encryption. For details on TEAV, visit: http://www.axlradius.com/freestuff/TEAV.java.

The JDBC driver supports RSA encryption. Each JDBC connection uses a unique RC4 session key to encode the users password for transport. The ADO.NET and ODBC drivers still use TEAV.

The TDV stores password hashes or encrypted passwords for users of the composite domain, but does not store passwords for LDAP or pass-through users.

TDV Command Line Utilities

The following TDV command line utilities make use of a -optfile or -configFile option, which can be used to hide password information from the command line:

- pkg_import.<sh | bat>
- pkg_export.<sh | bat>
- backup_import.<sh | bat>
- backup_export.<sh | bat>
- repo_util.<sh | bat>

Studio Session Security

For non-SSL session protection you can use the Studio Session Authentication configuration parameter. This configuration parameter adds an extra authentication level for session protection between the TDV Server and Studio for use with unencrypted connections. This parameter can be found in the TDV Studio client (goto Administration->Configuration and search for the parameter “studio session”) Navigate to the property Server->Configuration->Security->Authentication->Studio Session Authentication. Following are the values for this property. The default value is False.

- True—use session protection.
- False—don't use session protection.

Data Source Security

The following table describes how security is maintained between TDV and data sources.

Descriptions	8.0 and Following
Data source passwords encrypted and stored in the TDV metadata repository using:	AES
The TDV Server passes connection profile information to a vendor-supplied database driver, which encodes login and password according to vendor specifications and negotiates a secured session connection between the targeted database and the TDV Server.	Database driver encoding
Passwords in HTTP / SOAP headers during data source Web Service invocations are sent in the following formats:	Clear text, base64-encoded
Web Service security for data sources support.	Supported
Pass-through of incoming non-standard HTTP headers to data sources over HTTP.	Configured per header per data source
Web Service: NTLM authentication through an NTLM header.	Supported
Web Service: NTLM authentication through a Negotiate header.	Not supported
Web Service: Kerberos authentication through a Negotiate header.	Supported
Delegation/forwarding of client credentials to Kerberos data sources.	Supported for Sybase and Oracle thin drivers
Kerberos access to Sybase databases.	Supported
Kerberos access to MS SQL Server databases.	Supported. Not supported for data ship.
Kerberos access to Greenplum databases.	Supported
Kerberos access to Oracle databases.	11g drivers to 11g and 10g databases

Export Files Security

This section describes TDV password security for export files.

By default, data source passwords are excluded from the package export (CAR) files. When explicitly included, they are encrypted.

Data source passwords in package export directories are encrypted.

User passwords for users in the composite domain are encrypted and included in full server backup export (CAR) files, but they are not included by default in package export files. When users are included in the export file, the passwords are encrypted.

The repository password is included in full server backup export files, but not in package export files. When included, the repository password is encrypted.

The password for each LDAP domain (but not passwords for LDAP users) is included in full server backup export files, but not in package exports. When included, LDAP domain passwords are encrypted.

Monitor Security

Passwords in HTTP or SOAP headers for the following listed actions are encrypted using base64 encoding:

- Flush repository cache
- Get server list
- Get server status
- Stop monitor
- Start server
- Stop server
- Restart server

JDBC, ODBC, and ADO.NET Client Security

TDV provides the following security for communications with clients via JDBC or ODBC or ADO.Net..

Driver and Path	When	Encryption
JDBC programs to TDV	Performing TDV authentication during Create Connection process	RSA
JDBC programs to and from TDV, throughout connection	encrypt=true	Data encoded with TLS/SSL
JDBC programs to and from TDV	During connection	User password encoded with unique RC4 session key
ODBC programs to TDV	Performing TDV authentication during Create Connection process	TEAV
ADO.NET, throughout connection	During connection	TEAV

TDV supports the following Single Sign-On access:

Driver	SSO Access Through
JDBC	Kerberos
ODBC	Kerberos, NTLM
ADO.NET	Kerberos, NTLM

Manager Clients Security

Initial LDAP domain creation and update sends login and password from Manager to TDV as clear text.

Create and update LDAP domain connection profiles using a browser launched locally on the TDV installation.

Studio Client Security

Passwords sent from Studio to TDV during user authentication are encrypted.

Passwords sent between Studio and TDV during data source create or update processes are encrypted.

Passwords sent between Studio and TDV during domain create and update processes are not supported. Domain, group, and user management can be done using TDV Manager.

Passwords in HTTP/SOAP headers for the following actions are encrypted and base64-encoded:

- Flush Repository Cache
- Get Server List
- Get Server Status
- Start Server
- Stop Server
- Restart Server
- Fetch Logs

Single Sign-On access using Kerberos is supported.

TDV Server Security

In order to provide security from the host header attack, TDV provides a configuration option that users can tune. Navigate to the property Server-> Configuration-> Security-> Allowed Hosts. Sites mentioned in this list determines the allowed host/domain names.

A fake Host value in incoming HTTP request headers can be used for Cross-Site Request Forgery, cache poisoning attacks, and poisoning links in emails. This configuration determines the allowed host/domain names.

Values in this list can be fully qualified names (e.g. 'www.example.com'), in which case they will be matched against the request's Host header exactly (case-insensitive, not including port). A value beginning with a period can be used as a subdomain wildcard: '.example.com' will match example.com, www.example.com, and any other subdomain of example.com.

Default value is empty which means the Host header is not validated.

Changing this value will have no effect until the next server restart.

Web Service Client Security

TDV supports a variety of Web Service security standards. These are listed and explained in the following sections:

- Supported Web Service Security Standards, page 20
- Explanation of Web Services Policy, page 22

Supported Web Service Security Standards

TDV supports the following Web Service client security standards:

- Passwords in HTTP / SOAP headers during Web Service invocations to or from TDV Server in clear text, base64-encoded
- WS-Security for Web Service clients (next section)
- WSSE UsernameToken SOAP headers, used instead of transmitting usernames and passwords (composite domain only). For this to work, the Store User Password configuration parameter must be changed to True from its default setting of False.
- X-WSSE UsernameToken HTTP extension header instead of transmitting usernames and passwords (composite domain only)
- Use of WSSE and X-WSSE authentication require the server to be configured to store passwords in the repository rather than hash values.
- NTLM authentication through an NTLM header
- NTLM authentication through a Negotiate header
- Kerberos authentication through a Negotiate header

Data source Web Service invocations from TDV Server can support SSL with or without client authentication (if the data source supports SSL).

The following security policies, in the form of XML files, are provided for Web Service clients.

Transport or Standard	System Security Policy	Description
HTTP	Http-Basic-Authentication.xml	Policy that requires a user name and password when making a request.

Transport or Standard	System Security Policy	Description
HTTP	Http-UsernameToken-Digest.xml	Policy that validates against a UsernameToken header encrypted using a nonce value.
HTTP	Http-UsernameToken-Plain.xml	Policy that validates against a UsernameToken header. The password can be in plain text.
HTTPS	Https-Basic-Authentication.xml	Policy that requires a user name and password when making a request.
HTTPS	Https-ClientCertificateRequire.xml	Policy that requires client certificates.
HTTPS	Https-UsernameToken-Digest.xml	Policy that validates against a UsernameToken header encrypted using a nonce value.
HTTPS	Https-UsernameToken-Plain.xml	Policy that validates against a UsernameToken header. The password can be in plain text.
SOAP	UsernameToken-Digest.xml	Policy that validates against a UsernameToken header encrypted using a nonce value.
SOAP	UsernameToken-PlainText.xml	Policy that validates against a UsernameToken header. The password can be in plain text.
SAML	Saml1.1-Bearer-Wss1.1.xml	Method in which the bearer assertion is used to facilitate single sign-on to the web browser.
SAML	Saml1.1-HolderOfKey-Wss1.0.xml	Method that establishes a correspondence between a SOAP message and the SAML assertions added to the SOAP message.
SAML	Saml1.1-SenderVouches-Wss1.1.xml	Subject-confirmation method that enables an attesting entity to vouch for the identity of a subject to a party that trusts the sender.

Explanation of Web Services Policy

A Web Services policy is the same as an authentication scheme, but it is expressed in the form of an element in an XML file.

The XML snippet is referred to as a Web Services policy. The format of the XML snippet is described in Web Services Policy 1.2 - Framework (WS-Policy), which is at:

http://www.w3.org/Submission/WS-Policy/

This is the official specification, and the best source of reference for understanding policies.

Policies are server-side. The reason for selecting a policy is to tell the TDV server what authentication scheme to use when authenticating requests from clients.

TDV uses the Metro JDK to implement the authentication for each policy. Metro is documented at:

http://www.ibm.com/developerworks/java/library/j-jws10/index.html

Web policy basics are explained at:

http://www.ibm.com/developerworks/java/library/j-jws18/

Further information about Web Service policy can be found at:

- TDV Administrator Security Policy Actions, page 22
- SOAP Web Service Example, page 22
- REST Web Service Example, page 23

TDV Administrator Security Policy Actions

As TDV administrator, you need to select the policy that represents the desired authentication scheme. You do *not* need to:

- Modify the policies (for example, edit the XML policy element)
- Do anything except select a policy for the server side
- Do anything at all on the client side

SOAP Web Service Example

To select Basic Authentication for a SOAP Web Service, select the policy that represents the authentication scheme from the Security Policy drop-down list in the Service pane on the SOAP panel for the Web Service you are publishing. For a description of the procedure, see "Publishing a WSDL SOAP Data Service" or "Publishing a Contract-First WSDL SOAP Data Service" in the *TDV User Guide*.

REST Web Service Example

To select Basic Authentication for a REST Web Service, make sure Enable HTTP Basic is set to true in the Service pane on the REST panel for the Web Service you are publishing. For a description of the procedure, see "Publishing a WSDL REST Data Service" in the *TDV User Guide*.

Authentication between Clients and TDV

The table below lists the authentication protocols supported between clients and the TDV Server.

Authentication Protocol	TDV Support
Kerberos	Active
LDAP	Active
Kerberos for LDAP	Active
NTLM	Active

Using Kerberos Constrained Delegation

TDV JDBC driver can also be configured to use Kerberos Constrained Delegation. This feature allows a service to obtain service tickets to a restricted list of other services running on specific servers on the network after it has been presented with a service ticket. For more details on the process see: https://technet.microsoft.com/en-ca/library/cc995228.aspx.

The userGSSCredential connection property can be used in the connection URL to pass in a GSSCredential object. The following sample code shows how to use the property to pass the GSSCredential into the driver using JDBC:

```
GSSCredential impersonatedUserCredential = [userCredential]
Properties driverProperties = new Properties();
Driver driver = (Driver) Class.forName("cs.jdbc.driver.CompositeDriver").newInstance();
driverProperties.setProperty("authenticationMethod", "kerberos");
driverProperties.put("userGSSCredential", impersonatedUserCredential);
Connection conn = DriverManager.getConnection(CONNECTION_URL, driverProperties);

GSSCredential impersonatedUserCredential = [userCredential]
CompositeDataSource datasource = new CompositeDataSource();
datasource.setURL(CONNECTION_URL);
datasource.setUserGSSCredential(impersonatedUserCredential);
Connection conn = datasource.getConnection();
```

Authentication between TDV and Data Sources

The table below lists the authentication protocols supported between the TDV Server and data sources.

Authentication Protocol	TDV Support
Kerberos for IBM DB2 LUW v9.5	Active
Kerberos for MS SQL Server 2008 and 2012	Active
Kerberos for HiveServer2	Active
Kerberos for Oracle 10g	Active
Kerberos for Oracle 11g	Active
Kerberos for SOAP	Active
Kerberos for REST	Active
Kerberos for Sybase ASE v15	Active
Kerberos for WSDL	Active
Kerberos for XML over HTTP	Active
NTLM for REST	Active
NTLM for SOAP	Active
NTLM for WSDL	Active
NTLM for XML over HTTP	Active

Composite Domain Security

TDV supports its own security domain, and one can define users and groups in it. However, these users and groups do not exist outside the TDV environment. Many organizations use Microsoft Active Directory or an LDAP server to manage users and groups throughout the enterprise. TDV allows users to introspect those Active Directory and LDAP servers, and create security domains inside TDV for them.

Because the composite domain does not exist outside TDV, user passwords are either hashed or encrypted, and stored in the security_members table in the TDV metadata repository. Also note the following:

- TDV stores passwords for each user in the composite domain.
- TDV does not store passwords for Active Directory and LDAP domains. Instead, TDV forwards user credentials to the Active Directory server for user authentication.
- TDV does not store passwords for dynamic domain users.
- TDV supports case-sensitive user logins from external LDAP domains.
- TDV does not allow implicitly anonymous LDAP login through blank passwords.

SSL Protocol Configuration

In versions prior to TDV 7.0.8, TDV and Business Directory were configured to use only TLSv1 as the SSL protocol.

This means TDV clients using SSL will use TLSv1 as the default protocol. If you want to change this to a newer version of TLS (e.g. TLSv1.1 or TLSv1.2) then you will need to do the following configuration in your TDV and/or Business Directory instance.

TDV:

- Stop TDV (i.e. composite.sh/bat monitor stop).
  Note: if you see "-Dhttps.protocol" set, make sure you change it to "-Dhttps.protocols".
- Modify "-Dhttps.protocols" value in <INSTALL_DIR>/bin/composite_server.sh/bat to newer TLS value.
  Examples: "-Dhttps.protocols=TLSv1.1" or "-Dhttps.protocols=TLSv1.2"
  Note: If your installation uses JRE1.8 and -Dhttps.protocols option does not exist in the above script then you do not need to make any change. If your installation uses JRE1.8 and the above option exists then remove that option from the script. If your installation uses JRE1.7 then set the value explicitly to TLSv1.1 or TLSv1.2.
- Modify "-Dhttps.protocols" value in the "java.opts" section of <INSTALL_DIR>/conf/server/server.properties. Examples: "-Dhttps.protocols=TLSv1.1" or "-Dhttps.protocols=TLSv1.2"
- Start TDV and launch Studio. Open the Administration > Configuration... dialog and search for "Disable Protocols for SSL Connectors"

- Shutdown the server.
- Start TDV (i.e. composite.sh/bat monitor start)

Business Directory:

- Stop Business Directory (i.e. bd.sh/bat monitor stop).
  Note: if you see "-Dhttps.protocol" set, make sure you change it to "-Dhttps.protocols".
- Modify "-Dhttps.protocols" value in <INSTALL_DIR>/bin/bd_server.sh/bat to newer TLS value. Examples: "-Dhttps.protocols=TLSv1.1" or "-Dhttps.protocols=TLSv1.2"
  Note: If your installation uses JRE1.8 and -Dhttps.protocols option does not exist in the above script then you do not need to make any change. If your installation uses JRE1.8 and the above option exists then remove that option from the script. If your installation uses JRE1.7 then set the value explicitly to TLSv1.1 or TLSv1.2.
- Modify "-Dhttps.protocols" value in the "java.opts" section of <INSTALL_DIR>/bd/conf/server/server.properties. Examples: "-Dhttps.protocols=TLSv1.1" or "-Dhttps.protocols=TLSv1.2"
- Review Business Directory settings for "/server/communications/sslProtocolsToRemove"
- Start TDV and launch Studio.
- Open the Administration > Configuration... dialog and search for "Disable Protocols for SSL Connectors". Review the settings and make sure they reflect what you want.
- Shutdown the server.
- Start Business Directory (i.e. bd.sh/bat monitor start)

JRE Cipher Suite

TDV and Business Directory use JRE for all operating systems that these products support.

Some ciphers are not active unless the JRE has the Java Cryptograph Extensions downloaded and installed.

The JRE distributions default to the STRONG but limited cryptography policy files for the JCE framework.

For Oracle - Linux/Windows platforms (JRE 1.8)

An asterisk (*) indicates that the cipher in enabled by default

SSL_RSA_WITH_NULL_MD5

SSL_RSA_WITH_NULL_SHA

TLS_DH_anon_WITH_AES_128_CBC_SHA

TLS_DH_anon_WITH_AES_128_CBC_SHA256

TLS_DH_anon_WITH_AES_128_GCM_SHA256

TLS_DH_anon_WITH_AES_256_CBC_SHA

TLS_DH_anon_WITH_AES_256_CBC_SHA256

TLS_DH_anon_WITH_AES_256_GCM_SHA384

*TLS_DHE_DSS_WITH_AES_128_CBC_SHA

*TLS_DHE_DSS_WITH_AES_128_CBC_SHA256

*TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

*TLS_DHE_DSS_WITH_AES_256_CBC_SHA

*TLS_DHE_DSS_WITH_AES_256_CBC_SHA256

*TLS_DHE_DSS_WITH_AES_256_GCM_SHA384

*TLS_DHE_RSA_WITH_AES_128_CBC_SHA

*TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

*TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

*TLS_DHE_RSA_WITH_AES_256_CBC_SHA

*TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

*TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDH_anon_WITH_AES_128_CBC_SHA

TLS_ECDH_anon_WITH_AES_256_CBC_SHA

TLS_ECDH_anon_WITH_NULL_SHA

*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

*TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

*TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA

*TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
*TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_NULL_SHA
*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
*TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
*TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_NULL_SHA
*TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
*TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
*TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
*TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
*TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
*TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_NULL_SHA
*TLS_EMPTY_RENEGOTIATION_INFO_SCSV
*TLS_RSA_WITH_AES_128_CBC_SHA
*TLS_RSA_WITH_AES_128_CBC_SHA256
*TLS_RSA_WITH_AES_128_GCM_SHA256
*TLS_RSA_WITH_AES_256_CBC_SHA
*TLS_RSA_WITH_AES_256_CBC_SHA256
*TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_NULL_SHA256

For AIX platform (JRE 1.8)

An asterisk (*) indicates that the cipher in enabled by default
SSL_DHE_DSS_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA

SSL_DH_anon_WITH_AES_128_CBC_SHA

SSL_DH_anon_WITH_AES_128_CBC_SHA256

SSL_DH_anon_WITH_AES_128_GCM_SHA256

SSL_DH_anon_WITH_AES_256_CBC_SHA

SSL_DH_anon_WITH_AES_256_CBC_SHA256

SSL_DH_anon_WITH_AES_256_GCM_SHA384

SSL_DH_anon_WITH_DES_CBC_SHA

SSL_ECDHE_ECDSA_WITH_NULL_SHA

SSL_ECDHE_RSA_WITH_NULL_SHA

SSL_ECDH_ECDSA_WITH_NULL_SHA

SSL_ECDH_RSA_WITH_NULL_SHA

SSL_ECDH_anon_WITH_AES_128_CBC_SHA

SSL_ECDH_anon_WITH_AES_256_CBC_SHA

SSL_ECDH_anon_WITH_NULL_SHA

SSL_KRB5_WITH_DES_CBC_MD5

SSL_KRB5_WITH_DES_CBC_SHA

SSL_RSA_FIPS_WITH_DES_CBC_SHA

SSL_RSA_WITH_DES_CBC_SHA

SSL_RSA_WITH_NULL_MD5

SSL_RSA_WITH_NULL_SHA

SSL_RSA_WITH_NULL_SHA256

*SSL_DHE_DSS_WITH_AES_128_CBC_SHA

*SSL_DHE_DSS_WITH_AES_128_CBC_SHA256

*SSL_DHE_DSS_WITH_AES_128_GCM_SHA256

*SSL_DHE_DSS_WITH_AES_256_CBC_SHA

*SSL_DHE_DSS_WITH_AES_256_CBC_SHA256

*SSL_DHE_DSS_WITH_AES_256_GCM_SHA384

*SSL_DHE_RSA_WITH_AES_128_CBC_SHA

*SSL_DHE_RSA_WITH_AES_128_CBC_SHA256

*SSL_DHE_RSA_WITH_AES_128_GCM_SHA256

*SSL_DHE_RSA_WITH_AES_256_CBC_SHA
*SSL_DHE_RSA_WITH_AES_256_CBC_SHA256
*SSL_DHE_RSA_WITH_AES_256_GCM_SHA384
*SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
*SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
*SSL_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
*SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
*SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
*SSL_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
*SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA
*SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256
*SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256
*SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA
*SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384
*SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384
*SSL_ECDH_ECDSA_WITH_AES_128_CBC_SHA
*SSL_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
*SSL_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
*SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA
*SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
*SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
*SSL_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
*SSL_ECDH_RSA_WITH_AES_128_CBC_SHA
*SSL_ECDH_RSA_WITH_AES_128_CBC_SHA256
*SSL_ECDH_RSA_WITH_AES_128_GCM_SHA256
*SSL_ECDH_RSA_WITH_AES_256_CBC_SHA
*SSL_ECDH_RSA_WITH_AES_256_CBC_SHA384
*SSL_ECDH_RSA_WITH_AES_256_GCM_SHA384
*SSL_RSA_WITH_AES_128_CBC_SHA
*SSL_RSA_WITH_AES_128_CBC_SHA256

*SSL_RSA_WITH_AES_128_GCM_SHA256

*SSL_RSA_WITH_AES_256_CBC_SHA

*SSL_RSA_WITH_AES_256_CBC_SHA256

*SSL_RSA_WITH_AES_256_GCM_SHA384

*TLS_EMPTY_RENEGOTIATION_INFO_SCSV

How To Disable Specific Ciphers

If you want to disable specific ciphers you can modify the JRE as follows:

Edit <INSTALL_DIR>/jre/lib/security/java.security

jdk.tls.disabledAlgorithms=<ALGORITHMS>

JVM-wide algorithm restrictions for SSL/TLS processing. It is possible to disallow certain algorithms or limit key sizes.

These settings are available since Java 1.7. For more information on algorithms and usage, see this link: https://www.java.com/en/configure_crypto.html.