



# TIBCO® Graph Database Security Guidelines

*Version 3.1.0*

*November 2021*



# Contents

---

- About this Product ..... 3
  - Product Editions ..... 3
- TIBCO Documentation and Support Services ..... 4
- Security Features ..... 5
- Security Vulnerabilities ..... 6
- Product Connectivity ..... 7
- Data Security and Privacy ..... 9
- Developing Secure Applications ..... 10
- TIBCO® Graph Database Security: Task for Administrators ..... 11
  - Roles and Responsibilities ..... 11
  - Coordination ..... 11
  - Database Security ..... 12
  - Securing Server ..... 14
  - Securing Application ..... 15
- Appendix A – Database Configuration File ..... 16
- Appendix B – Server Configuration File ..... 17
- Appendix C – IANA RFC Cipher name to OpenSSL Names ..... 18
- Legal and Third-Party Notices ..... 19

# About this Product

---

TIBCO® is proud to announce the latest release of TIBCO® Graph Database software.

This release is the latest in a long history of TIBCO products that leverage the power of Information Bus® technology to enable truly event-driven IT environments. To find out more about how TIBCO® Graph Database software and other TIBCO products are powered by TIB® technology, please visit us at [www.tibco.com](http://www.tibco.com).

## Product Editions

TIBCO® Graph Database is available in a community edition and an enterprise edition.

TIBCO® Graph Database - Community Edition is ideal for getting started with TIBCO Messaging, for implementing application projects (including proof of concept efforts), for testing, and for deploying applications in a production environment. Although the community license limits the number of production processes, you can easily upgrade to the enterprise edition as your use of the database expands.

The community edition is available free of charge. It is a full installation of the TIBCO® Graph Database software, with the following limitations and exclusions:

- Runs as a Standalone server with Active-Passive fault-tolerance mode.
- Maximum of 5 connections and 5 named users with a maximum database storage capacity of 100 GB.
- Users do not have access to TIBCO Support, but you can use the TIBCO community as a resource. (<https://community.tibco.com>)

TIBCO® Graph Database – Community Edition has the following additional limitations and exclusions.

- Excludes Clustering of database instance for High Availability and Scalability.
- Excludes Multi-tenancy.

TIBCO® Graph Database – Enterprise Edition is ideal for all application development projects, and for deploying and managing applications in an enterprise production environment. It includes all features presented in this documentation set, as well as access to TIBCO Support.

## Product Editions

# TIBCO Documentation and Support Services

---

## How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in 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>.

## Product-Specific Documentation

Documentation for TIBCO Graph Database is available on <https://docs.tibco.com/products/tibco-graph-database-enterprise-edition-3-0-0> page.

This feature is available to both Enterprise edition and Community. The guidelines specified for Clustering is applicable only to Enterprise edition.

The following documents form the documentation set:

- *TIBCO® Graph Database Getting Started*: Read this manual before reading any other manual in the documentation set. This manual describes the terminology and concepts of the platform. The other manuals in the documentation set assume you are familiar with the information in this manual.
- *TIBCO Graph Database Administration* : Read this manual to learn how to manage the runtime and deploy and manage applications.
- *TIBCO® Graph Database Security Guidelines*: Read this manual to learn more about security guidelines and recommendations for TIBCO® Graph Database.
- *TIBCO Graph Database Release Notes*: Read this manual for a list of new and changed features, steps for migrating from a previous release, and lists of known issues and closed issues for the release.

## How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit <http://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>.

# Security Features

---

This document describes guidelines to ensure security within the various components of the TIBCO® Graph Database, the channels of communication between them, and also secure the data and access within the database. It also provides additional security-related guidance and recommendations for other aspects of internal and external communication. In particular, this document provides details of product connectivity, access, and configuration of security options.

For information about how to upgrade third-party components and post-installation activities, see *TIBCO® Graph Database Getting Started*.

TIBCO® Graph Database includes the following security features.

- Secure transports for communication between client and server, proxies.
- TLSv1.2+ to secure TCP transports.
- Authentication and Authorization services.
- Access control policies on data.
- Securing sensitive and confidential data with access policies.
- Isolation & Containerization.

# Security Vulnerabilities

---

This topic describes the key security technologies for TIBCO® Graph Database software. In addition to these key technologies, security also depends in part upon correct configuration and uses of its component and capabilities.

## OpenSSL

Security features that protect TIBCO® Graph Database connections and communications, Encrypting/Decrypting data depend on the implementation of OpenSSL. If the security of OpenSSL were compromised, TIBCO® Graph Database and applications that use the database could be vulnerable as well.

## Python

TIBCO® Graph Database supports Stored Procedures written in Python. It can use python libraries and third-party libraries as per application needs. This code needs to go through proper review procedures to ensure of handling sensitive data, external communications, and other security vulnerabilities; just like one would review an application written for Graph Database. TIBCO® Graph Database ships white-listed Python libraries, and it depends on its security.

## Operating System

TIBCO® Graph Database runs on top of an Operating System and depends on its security. If the security of the OS is compromised, TIBCO® Graph Database and applications that use the database could be vulnerable as well.

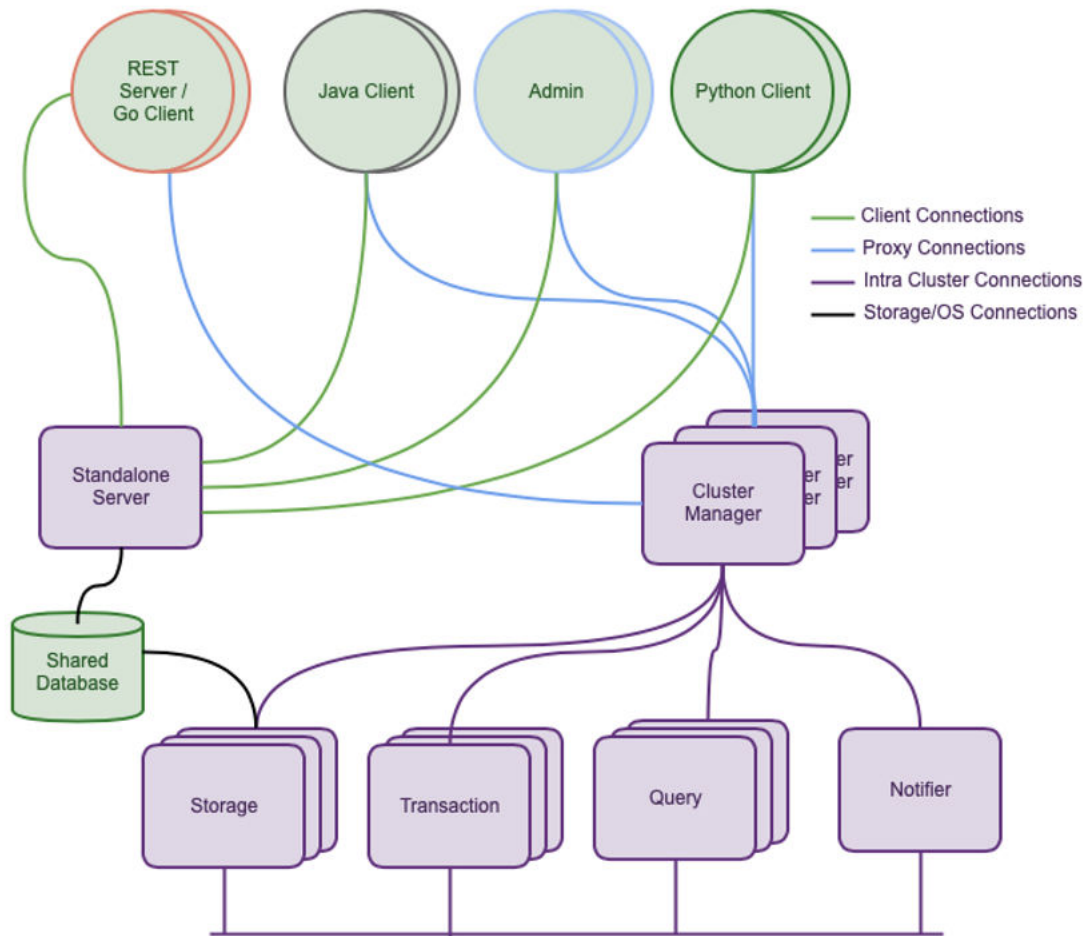
## Storage System

TIBCO® Graph Database uses storage provided by Operating System or a Storage Area Network or Network File System and depends on its security. If the security of the Storage system is compromised, TIBCO® Graph Database and applications that use the database could be vulnerable as well.

# Product Connectivity

TIBCO® Graph Database includes several interconnecting components and also connects with other TIBCO and third-party products. You can secure all connections within the TIBCO® Graph Database.

*Connections among TIBCO® Graph Database components and applications*







The diagram depicts a variety of components and other processes that communicate within a Graph Database ecosystem. (To simplify the diagram, the diagram omits redundant connections to duplicate processes).

This document addresses the security issues, that arise for each type of connection; and the actions you must take to ensure security.

The minimum viable secure deployment includes at least one Standalone Server, 2 Clients (including Admin), and a database segment on the OS filesystem. The minimum secure deployment for a Cluster is 1 Cluster Manager & 3 Agents, and 2 Clients.

The following table shows what the communication channel supports, and documentation will guide you to secure the same.

Key	Channel	TCP	SSL
	Client Connections	√	√
	Proxy Connections	√	√
	Intra-Agents	√	X
	Storage/OS	√, Proprietary	X

Client and Proxy channels can have more than 1 TCP and SSL transports. Transport choice is a function of application needs. An application that needs high throughput and runs behind a firewall in a data center and is localized within a subnet can choose TCP, whilst the need of securing the channel for any promiscuous sniffing requires the channel to be encrypted and will choose SSL. This document guides the user to configure the channel for Secured Transport.

Both the transports (SSL, and plain TCP) uses binary encoding such as ASN.1 DER encoding for efficient and fast transport of data.



# Data Security and Privacy

---

TIBCO® Graph Database persists data and relationships as nodes and edges in segments (files) on storage systems provided by the Operating System. Portions of data can be subject to confidentiality and personal in nature. Furthermore, access to data (including PII and confidential) requires proper authorization and access control policies in place.

TIBCO® Graph Database provides encrypting data at a field-level. It provides AAA (Authentication, Authorization and Auditing) services.

This document guides the user on how to configure databases to store confidential and PII data, and to setup Access-control policies.

An auditing is not provided out of the box, but can be implemented by application with the use of Triggers in Database.

# Developing Secure Applications

---

Security is everyone's business, and everyone needs to collaborate and coordinate the requirements, tasks. This section can be used as a checklist for Application Developers, Database Administrator, and the office of CISO - Security Administrator.

Users may perform one or more roles (such as Application Developers, and Database Administrator).

## Pre-requisites

The application developer, database administrator, security administrator have coordinated to exchange security-related information and artifacts. See Coordination. User can use this as a template checklist as a base form.

## Checklists

The administrator or the developer needs to perform & verify the following tasks:

1. Coordinate security details with Security team with respect to the cipher suite, bit strength, algorithm to use, and other features.
2. Secure the Database
  - a. Record the System user and password.
  - b. Coordinate the Security encryption and decryption keys with the security administrator.
  - c. Coordinate with the Database administrator, Business owner and Security to identify the fields that need to be secure, and its access policy.
3. Securing the Server
  - a. Secure the Net Listener on Server to listen on Secured Sockets for sensitive and confidential transmission.
  - b. Consider Multi-tenancy to isolate/partition data for different Entities, when data security is needed, and resources have to be utilized efficiently.
  - c. Consider Containerization when utmost security is needed i.e. Data partitioning and resource isolation.
4. Client Applications
  - a. Application developers should ensure they have the correct transport protocol and URL specified in the connection string.
  - b. Using a password as plain text, consider using the obfuscation tool.
  - c. `"ssl://scott@localhost:8223/{dbName=inventory;}";`

Once Database security is defined, it cannot be changed for the lifetime of the database. If you need to change it, export the database, then re-initialize the database with new keys, and reimport the data from the exported files.

The appendix A, and B provides template checklist form for user's convenience.

# TIBCO® Graph Database Security: Task for Administrators

## Roles and Responsibilities

The following table defines roles and responsibilities. Your organization might have a different name, and combined responsibility. The Acronyms used in the document convey the responsibilities as intended in the below section.

Roles	Responsibilities
Database Administrator (DBA)	Manages and model's database. Ensures data integrity and consistency.
Security Administrator (SA)	Manages and enforces corporate wide security standard. Defines the right Cipher Suite to use, the channel's that need to be encrypted, and also identifies the PII and Confidential data elements.
Site Reliability Engineer (SRE)	Manages the life cycle of application and various components. Manages data backup and other aspects of the application.
Application Developer (Dev)	Responsible in developing the application, and tailoring it to the business rules. Follows secured programming practices as setup by the corporate governance.

## Coordination

To secure a system that uses TIBCO® Graph Database software, administrators and application developers must coordinate to share security requirements and artifacts. This topic highlights the artifacts and information that pertain to security.

TIBCO® Graph Database does a self-signed certificate with customizable parameters provided by the System Administrator. The parameters described below are used for Database Security and Transport Security.

1. Cipher Suite. Administrator will choose a Cipher Suite that is consistent with the Corporate System Security Requirement. See Appendix C for Cipher Suite names.
  - a. Cipher Name is a TLS 1.2 Name obtained from IANA Registry.
  - b. <https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4>
2. Cipher Strength. Some Ciphers like the Diffie-Hellman Cipher Suites require minimum bit length to use for their algorithm to produce strong keys. Coordinate with your administrator to generate strong keys consistent with the Corporate System Security Requirement.
3. Cipher Curve. For an Elliptic Curve based Cipher, a curve name must be provided.
4. Expiry Interval. This parameter is used when the Cipher Suite is used to generate a dynamic certificate for SSL Transport negotiations.
5. System User and Password. For every database, a system user and password must be provided. This user has all the privileges to the database.

## Database Security

Data security is of vital importance to a business function. Database administrator in collaboration with business and security administrator, identify the sensitive and confidential data elements that need to be secure from storage and access point of view. This section will guide the user with the necessary procedure.

### Prerequisites

1. Responsible parties have coordinated with Security information. See Coordination.
2. The database administrator has the model and identified the fields to be encrypted.
3. The database administrator has all the enterprise users who will access the data, and their respective roles and responsibilities.

### Procedure

1. Create/Modify a database configuration file. Under the security section, fill in the values provided by your Security Administrator. See the Figure below. *Database security configuration*

```
# Default Security configuration.
# The syscipher is used for creating a System-Wide Self Signed Database certificate.
# The Database certificate provides private/public encryption Keys.
# The cipher name is a TLS 1.2 Cipher Name obtained from IANA Registry.
# See https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4
# It can be obtained by running
# $> openssl ciphers -V -tls1_2 -stdname|
# The properties for security are as follows
# Applicability : Initialization
# sysuser       : The system user name for the database. The default name is admin
# syspasswd     : The system user password for the database. The default password is admin
# sysciphersuite : System wide Cipher to be used for TLS and encrypted field, and password.
# syscipherbits  : For DH type the bit strength to use. Minimum is 256.
# sysciphercurve : EC curve name if it is EC based Cipher Suite
[security]
sysuser       = admin
syspasswd     = admin
sysciphersuite = AES256-SHA256
syscipherbits  = 1024
sysciphercurve = secp521r1
```

2. For each field that is marked confidential or sensitive by the Business Owners, perform one of the 2 things.
  - a. Mark the field in the configuration file as encrypted. See below.

```
[attrtypes]
name      = @type:string
desc      = @type:string
address   = @type:string
ssn       = @type:string @encrypted
networth  = @type:number(20,5) @encrypted
age       = @type:int
```

- b. Use the admin command to create the attribute as an encrypted attribute. Ensure you are logged in as an Administrator or as a user who has the privilege to modify the system catalogue.

```
admin@localhost:8223>create encrypted attrdesc salary as Double
Successfully created the attribute descriptor salary!
admin@localhost:8223>describe salary
Type: Attribute Descriptor
Name: salary
SysId: 9253
Attribute Type: Double
Array: N
Encrypted: Y
```

- c. Attribute descriptor cannot be dropped from system.
3. Create Roles and grant privilege to the system catalogue objects in the database. Similar to point 2, Roles can be created either in database configuration file or from admin console.

- a. In the database configuration, add roles as follows

```
[roles]
basicrole = @privs:g @perms:crudx|basicedge|basicnode,crx|all
userplus = @perms:crudx|all
```

- b. Use the admin command to add roles.

```
admin@localhost:8223>create role analyst with permission crude on types (all)
Successfully created the role analyst!
admin@localhost:8223>describe analyst
Type: Role
Name: analyst
SysID: 9258
Privileges:
System Catalog Permissions:
Default Permissions: crude
  Name      SysID  Granted  Revoked
admin@localhost:8223>
```

4. Create Users with specified roles and/or add Roles to an existing user. It is achieved similar to the way roles are added to the system. Skipping the screenshots for the same.
5. Choose passwords for the user. The password is digested using the PBKDF2 algorithm with SHA1 digest.
6. Ensure the correct user has the "Read/Update/Delete" permission on the \$SYSCATALOG object. This is a system table and provides access to view/delete system objects.
7. Ensure Operators who perform a backup of the database have Import/Export permissions on all objects.
8. Ensure Operators who monitor and manage the server instance have "Diagnostic" permission and Operator role permission. This allows operators to perform,
  - a. Dump server stack trace
  - b. Stop server
  - c. Show and kill connections
  - d. Get Monitoring Statistics
9. When the user leaves the organization, follow up by disabling/dropping the user, and backing up the user pertaining data.

## Securing Server

TIBCO® Graph Database provides both Clustering and Non-Clustering (Standalone) to host one or more databases for client applications. It can run as a group of coordinate agents on cooperative homogeneous machines on a network, or on a single machine as a Standalone Server. Either way it provides a channel to the client application and acts as a gateway intercepting requests to perform Transactions, Queries, System Management, and so on. Application and Corporate IT governance could require these channels to be secure and protected. This section guides the user with the necessary steps.

### Prerequisites

1. SRE has coordinated with the Security information. See Coordination.
2. SRE has created a server configuration or a cluster configuration.
3. SRE has identified the number of channels (net listeners) needed for the server based on the following criteria.
  - a. Functional Isolation - Isolate OLTP requests to OLAP requests
  - b. Throughput requirements
  - c. sensitivity requirements
  - d. Allocate 1 extra secured channel for Administrative purpose

### Procedure

1. For each channel, configure the [net listener] section as shown in figure.

```
# Netlistener configuration. Configure listen port for Database server
# name : A logical name for the netlistener. Mandatory
# host : The host name, ip number, or interface name it is bound to.
# port : Listening TCP port. Default is 8222 for StandAlone, 8225 for Cluster
# ssl : Enable SSL communication on this netlistener.
# sslTimeout      : SSL HandShake Timeout in sec. Range between [0..60].
# sslciphersuite  : Cipher suite to be used for TLS.
# sslcipherbits   : For DH type the bit strength to use. Minimum is 256.
# sslciphercurve  : EC curve name if it is EC based Cipher Suite
# sslcipherexpiry: Expire and regenerate the certificate dynamically.

[netlistener]
name      = analytics
host      = ::
port      = 8223
ssl       = true
sslTimeout = 10
sslciphersuite = AES256-SHA256
sslcipherbits = 1024
sslciphercurve = secp521r1
sslcipherexpiry = 1
```

2. For cluster configuration, Intra-Agent communications are only TCP based. Isolate the network either by interfaces (multi-homed machines) or by virtual segmentation for securing the data movement between the agents.

```
# Multi Tenancy :Specify the databases that this server manages.
# Format is name = configfile where name is name of the database and
#               configfile is the database configuration file.
# For EE the maximum of database depends on the System resources.
# For CE, Only 1 database can be managed.
[databases]
demodb = ./demodb.conf
#routesdb = ../examples/routes/routesdb.conf
#tracedb = ../examples/trace/tracedb.conf
#housedb = ../examples/hierarchy/housedb.conf
```

3. To host Multi-tenants on the Cluster or Non-Cluster server, add the database names and the path to the configuration file to the [databases] section.
4. Always run Admin console on SSL channel for secured communication. Using “tcp” as a protocol will raise a warning.

```
NOTE: Enter help for additional information. Ctrl-C quits the current prompt, Ctrl-D exits the
TGDB Admin Console.

Connect to URL (default is ssl://localhost:8223):tcp://localhost:8222
Login database name (default is demodb):
Login username (default is admin):
Login password (default is not shown):
Using insecure tcp connection instead of ssl. Should only use for testing purposes or behind a secure firewall. This is not recommended!
Connected successfully to database demodb hosted on server at tcp://admin@localhost:8222
admin@localhost:8222>
```

## Securing Application

Applications use Client API provided by TIBCO® Graph Database software. There are 3 necessary steps that every application developer should be aware of.

1. Secure communication between client and server requires the protocol to be specified as "ssl". The communication is ssl over TCP.
2. The URL should specify the database name it wishes to connect to. Do not use any default database name
3. The URL or connect API method should pass the user name and password. (If password is in plain text, use the obfuscation tool).

```
private void connect() throws Exception
{
    String url = "ssl://tgdb.metis.io:8222/{dbName=metisdb}";
    String user = "scott";
    String pwd = "scott";
    TGProperties props = TGEnvironment.getInstance().getAsSortedProperties();
    conn = TGConnectionFactory.getInstance().createConnection(url, user, pwd, props);
    conn.connect();
    initConnection();
}
```

# Appendix A – Database Configuration File

Database Config Name: \_\_\_\_\_ Date: \_\_\_\_\_

☐ Security Details Coordinated. Enter the values for all security related field in [security] section

Security Details					
Key	Value				
sysuser					
syspasswd	[*****]				
sslciphersuite					
sslcipherbits					
sslciphercurve					
sslcipherexpiry					
Role Details					
Role Name					
TypeName	Permissions				
	Create	Read	Update	Delete	Execute
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Role Name					
TypeName	Permissions				
	Create	Read	Update	Delete	Execute
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
User Details					
User Name		Role Name(s)			



# Appendix B – Server Configuration File

Server Config Name: Date:

- ☐ Security Details Coordinated. Enter the values for all security related field.
- ☐ Net listener Details [Repeat this for N listener]

Net Listener Name	Type	Details	
[Name1]	<input type="checkbox"/> SSL	Key	Value
	<input type="checkbox"/> Intra-Agent	Host	
	<input type="checkbox"/> Admin Console	Port	
		<input type="checkbox"/> IPv6	
		<input type="checkbox"/> Public	
		Notes	
Fill this if SSL is enabled		ssliphersuite	
		sslcipherbits	
		sslciphercurve	
		sslcipherexpiry	
[Name2]	<input type="checkbox"/> SSL	Key	Value
	<input type="checkbox"/> Intra-Agent	Host	
	<input type="checkbox"/> Admin Console	Port	
		<input type="checkbox"/> IPv6	
		<input type="checkbox"/> Public	
		Notes	
Fill this if SSL is enabled		ssliphersuite	
		sslcipherbits	
		sslciphercurve	
		sslcipherexpiry	

# Appendix C – IANA RFC Cipher name to OpenSSL Names

Output of command

```
$>./openssl cipher -v -tls1_2 -stdname
```

CodeId	Iana Name	OpenSSL	Ver	Kx	Au	En	Bits#	MAC
0x13,0x02	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	TLSv1.3	any	any	AESGCM	256	AEAD
0x13,0x03	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	TLSv1.3	any	any	CHACHA20/POLY1305	256	AEAD
0x13,0x01	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	TLSv1.3	any	any	AESGCM	128	AEAD
0xC0,0x2C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDSA-ECDHE-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM	256	AEAD
0xC0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDSA-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM	256	AEAD
0x00,0x9F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	TLSv1.2	DH	RSA	AESGCM	256	AEAD
0xCC,0xA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDSA-ECDHE-CHACHA20-POLY1305	TLSv1.2	ECDH	ECDSA	CHACHA20/POLY1305	256	AEAD
0xCC,0xA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDSA-RSA-CHACHA20-POLY1305	TLSv1.2	ECDH	RSA	CHACHA20/POLY1305	256	AEAD
0xCC,0xA7	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	TLSv1.2	DH	RSA	CHACHA20/POLY1305	256	AEAD
0xC0,0x2B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDSA-ECDHE-AES128-GCM-SHA256	TLSv1.2	ECDH	ECDSA	AESGCM	128	AEAD
0xC0,0x2F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDSA-RSA-AES128-GCM-SHA256	TLSv1.2	ECDH	RSA	AESGCM	128	AEAD
0x00,0x9E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	TLSv1.2	DH	RSA	AESGCM	128	AEAD
0xC0,0x24	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDSA-ECDHE-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES	256	SHA384
0xC0,0x28	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDSA-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES	256	SHA384
0x00,0x6B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	TLSv1.2	DH	RSA	AES	256	SHA256
0xC0,0x23	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDSA-ECDHE-AES128-SHA256	TLSv1.2	ECDH	ECDSA	AES	128	SHA256
0xC0,0x27	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDSA-RSA-AES128-SHA256	TLSv1.2	ECDH	RSA	AES	128	SHA256
0x00,0x67	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	TLSv1.2	DH	RSA	AES	128	SHA256
0xC0,0x0A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDSA-ECDHE-AES256-SHA	TLSv1	ECDH	ECDSA	AES	256	SHA1
0xC0,0x14	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDSA-RSA-AES256-SHA	TLSv1	ECDH	RSA	AES	256	SHA1
0x00,0x39	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	SSLv3	DH	RSA	AES	256	SHA1
0xC0,0x09	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDSA-ECDHE-AES128-SHA	TLSv1	ECDH	ECDSA	AES	128	SHA1
0xC0,0x13	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDSA-RSA-AES128-SHA	TLSv1	ECDH	RSA	AES	128	SHA1
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	SSLv3	DH	RSA	AES	128	SHA1
0x00,0xAD	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384	RSA-PSK-AES256-GCM-SHA384	TLSv1.2	RSAPSK	RSA	AESGCM	256	AEAD
0x00,0xAB	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	DHE-PSK-AES256-GCM-SHA384	TLSv1.2	DHEPSK	PSK	AESGCM	256	AEAD
0xCC,0xAE	TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256	RSA-PSK-CHACHA20-POLY1305	TLSv1.2	RSAPSK	RSA	CHACHA20/POLY1305	256	AEAD
0xCC,0xA1	TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256	DHE-PSK-CHACHA20-POLY1305	TLSv1.2	DHEPSK	PSK	CHACHA20/POLY1305	256	AEAD
0xCC,0xAC	TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256	ECDSA-PSK-CHACHA20-POLY1305	TLSv1.2	ECDEHPK	PSK	CHACHA20/POLY1305	256	AEAD
0x00,0x9D	TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	TLSv1.2	RSA	RSA	AESGCM	256	AEAD
0x00,0xA9	TLS_PSK_WITH_AES_256_GCM_SHA384	PSK-AES256-GCM-SHA384	TLSv1.2	PSK	PSK	AESGCM	256	AEAD
0xCC,0xAB	TLS_PSK_WITH_CHACHA20_POLY1305_SHA256	PSK-CHACHA20-POLY1305	TLSv1.2	PSK	PSK	CHACHA20/POLY1305	256	AEAD
0x00,0xAC	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256	RSA-PSK-AES128-GCM-SHA256	TLSv1.2	RSAPSK	RSA	AESGCM	128	AEAD
0x00,0xA8	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	DHE-PSK-AES128-GCM-SHA256	TLSv1.2	DHEPSK	PSK	AESGCM	128	AEAD
0x00,0x9C	TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	TLSv1.2	RSA	RSA	AESGCM	128	AEAD
0x00,0xA8	TLS_PSK_WITH_AES_128_GCM_SHA256	PSK-AES128-GCM-SHA256	TLSv1.2	PSK	PSK	AESGCM	128	AEAD
0x00,0x3D	TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	TLSv1.2	RSA	RSA	AES	256	SHA256
0x00,0x3C	TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	TLSv1.2	RSA	RSA	AES	128	SHA256
0xC0,0x38	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384	ECDSA-PSK-AES256-CBC-SHA384	TLSv1	ECDEHPK	PSK	AES	256	SHA384
0xC0,0x36	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA	ECDSA-PSK-AES256-CBC-SHA	TLSv1	ECDEHPK	PSK	AES	256	SHA1
0xC0,0x21	TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA	SRP-RSA-AES-256-CBC-SHA	SSLv3	SRP	RSA	AES	256	SHA1
0xC0,0x20	TLS_SRP_SHA_WITH_AES_256_CBC_SHA	SRP-AES-256-CBC-SHA	SSLv3	SRP	SRP	AES	256	SHA1
0x00,0xB7	TLS_RSA_PSK_WITH_AES_256_CBC_SHA384	RSA-PSK-AES256-CBC-SHA384	TLSv1	RSAPSK	RSA	AES	256	SHA384
0x00,0xB3	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384	DHE-PSK-AES256-CBC-SHA384	TLSv1	DHEPSK	PSK	AES	256	SHA384
0x00,0x95	TLS_RSA_PSK_WITH_AES_256_CBC_SHA	RSA-PSK-AES256-CBC-SHA	SSLv3	RSAPSK	RSA	AES	256	SHA1
0x00,0x91	TLS_DHE_PSK_WITH_AES_256_CBC_SHA	DHE-PSK-AES256-CBC-SHA	SSLv3	DHEPSK	PSK	AES	256	SHA1
0x00,0x35	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	SSLv3	RSA	RSA	AES	256	SHA1
0x00,0xAF	TLS_PSK_WITH_AES_256_CBC_SHA384	PSK-AES256-CBC-SHA384	TLSv1	PSK	PSK	AES	256	SHA384
0x00,0x8D	TLS_PSK_WITH_AES_256_CBC_SHA	PSK-AES256-CBC-SHA	SSLv3	PSK	PSK	AES	256	SHA1
0xC0,0x37	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256	ECDSA-PSK-AES128-CBC-SHA256	TLSv1	ECDEHPK	PSK	AES	128	SHA256
0xC0,0x35	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA	ECDSA-PSK-AES128-CBC-SHA	TLSv1	ECDEHPK	PSK	AES	128	SHA1
0xC0,0x1E	TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA	SRP-RSA-AES-128-CBC-SHA	SSLv3	SRP	RSA	AES	128	SHA1
0xC0,0x1D	TLS_SRP_SHA_WITH_AES_128_CBC_SHA	SRP-AES-128-CBC-SHA	SSLv3	SRP	SRP	AES	128	SHA1
0x00,0xB6	TLS_RSA_PSK_WITH_AES_128_CBC_SHA256	RSA-PSK-AES128-CBC-SHA256	TLSv1	RSAPSK	RSA	AES	128	SHA256
0x00,0xB2	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256	DHE-PSK-AES128-CBC-SHA256	TLSv1	DHEPSK	PSK	AES	128	SHA256
0x00,0x94	TLS_RSA_PSK_WITH_AES_128_CBC_SHA	RSA-PSK-AES128-CBC-SHA	SSLv3	RSAPSK	RSA	AES	128	SHA1
0x00,0x90	TLS_DHE_PSK_WITH_AES_128_CBC_SHA	DHE-PSK-AES128-CBC-SHA	SSLv3	DHEPSK	PSK	AES	128	SHA1
0x00,0x2F	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	SSLv3	RSA	RSA	AES	128	SHA1
0x00,0xAE	TLS_PSK_WITH_AES_128_CBC_SHA256	PSK-AES128-CBC-SHA256	TLSv1	PSK	PSK	AES	128	SHA256
0x00,0x8C	TLS_PSK_WITH_AES_128_CBC_SHA	PSK-AES128-CBC-SHA	SSLv3	PSK	PSK	AES	128	SHA1

## Legal and Third-Party Notices

---

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 DOCUMENT 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 DOCUMENT 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 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, the TIBCO logo, the TIBCO O logo, and Graph Database 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.txt file for the availability of this software version on a specific operating system platform.

THIS DOCUMENT 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 DOCUMENT 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 DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT 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.

This and other products of TIBCO Software Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (<https://www.tibco.com/patents>) for details.

Copyright © 2021. TIBCO Software Inc. All Rights Reserved.