TIBCO® Vault Server

Installation Guide

Software Release 2.0.1
August 2015

Two-Second Advantage®

TIBCO™

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 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 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.

TIBCO, The Power of Now, Two-Second Advantage, TIBCO Managed File Transfer, TIBCO Managed File Transfer Command Center, TIBCO Managed File Transfer Internet Server, TIBCO Managed File Transfer Internet Server with RocketStream, TIBCO Managed File Transfer Platform Server, TIBCO Managed File Transfer Platform Server Agent, Slingshot, and TIBCO Vault are either registered trademarks or trademarks of TIBCO Software Inc. or its subsidiaries 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.

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.

TIBCO® Managed File Transfer Internet Server with RocketStream® Accelerator is entitled TIBCO® Managed File Transfer Internet Server in certain other product documentation and in user interfaces of the product.

Contents

Preface

This guide explains how to install TIBCO Vault.

Topics

Related Documentation

This section lists documentation you may find useful.

TIBCO Vault Documentation

The following documents form the TIBCO Vault documentation set which can be viewed and downloaded from https://docs.tibco.com/products/tibco-vault-2-0-1 :

- *TIBCO Vault 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.
- *TIBCO Vault Installation Guide* Read this manual for instructions on site preparation and installation.
- *TIBCO Vault Administrator Guide* Read this manual for instructions on configuring the TIBCO Vault Server after the installation.
- *TIBCO Vault User Guide* Read this manual for instructions on using the product to perform file transfer requests and more with TIBCO Vault browser and Outlook Plug-in interfaces.
- *TIBCO Vault Quick Start Guide* Read this manual to view the most common setup configurations once you have installed the product and to read step-by-step instructions to setup common transactions.

How to Contact TIBCO Customer Support

For comments or problems with this manual or the software it addresses, contact TIBCO Support, as follows:

- For an overview of the TIBCO Support and information on getting started with TIBCO Support, visit http://www.tibco.com/services/support
- If you already have a valid maintenance or support contract, visit https://support.tibco.com

  Entry to this site requires a user name and password. If you do not have login credentials, click Register with Support.
- Technical Support email address support@tibco.com
- Technical Support Call Centers:
  - North and South America: +1.650.846.5724 or +1.877.724.8227 (1.877.724.TACS)
  - EMEA (Europe, Middle East, Africa): +44 (0) 870.909.3893
  - Australia: +61.2.4379.9318 or 1.800.184.226
  - Asia: +61 2 4379 9318

Installation

This section explains what is needed to successfully install TIBCO Vault Server.

Topics

- *System Requirements*
- *Installation Procedure*

System Requirements

Please note that support is provided for TIBCO Vault only when used with an indicated third party vendor's generally supported release versions. Once the operating system or other software component goes into extended support mode, or the vendor no longer supports a version, it will cease to be supported by TIBCO Technical Support. Please see the following sections for additional information on supported operating system, database system, Java, and other software components.

Minimum Operating System Version

One of the following minimum operating systems level or above that runs the appropriate Java version (see section C) and is supported by the vendor:

- HP HP-UX
  11i v1 (B.11.11), 11i v2 (B.11.23), 11i v3 (B.11.31) 64-bit on Itanium
- IBM AIX
  6.1, 7.1 64-bit on pSeries
- Microsoft Windows
  7 , 7 SP1, 8, Vista, XP 64-bit on x86-64
- Microsoft Windows Server
  2008 R2 SP1, 2008 SP2, 2012 64-bit 64-bit on x86-64
- Novell SUSE Linux Enterprise Server
  9.x, 10.x, 11.x 64-bit on x86-64
  10.x, 11.x 32-bit on x86-64
- Red Hat Enterprise Linux Server
  5.x, 6.x 64-bit on x86-64

Windows XP Service Pack 2, Windows 2000 Server and Professional, and Windows 2003 Server R2 reached end of mainstream support in July, 2010. Customers should migrate to supported versions of Windows Client

and Windows Server because in the event that you encounter an issue/outage in your environment on an unsupported product, Microsoft engineers may not be able to help resolve the issue until you've upgraded to a supported level.

Minimum Database

A database created on one of the following supported databases:

Note: Databases for TIBCO Vault should support a UTF-8 character set and have a case insensitive collation.

- **Microsoft SQL Server 2008 R2, 2008.x, 2012** (Using either Windows or SQL Authentication) - Customers must provide the MSSQL JDBC driver. The driver can be downloaded from http://sourceforge.net/projects/jtds/files/. Supported database driver is jTDS 1.3.1. Note: There are two zip files you can download, jtds-1.3.1-src.zip and jtds-1.3.1-dist.zip. Download the distribution file, jtds-1.3.1-dist.zip, and place it in a temporary directory. Extract all the files and verify jtds-1.3.1.jar is there.
- **MySQL 5.5.x** - Customers must provide the MySQL JDBC driver. The driver can be downloaded from http://ftp.plusline.de/mysql/Downloads/Connector-J/. Supported database drivers are v5.1.21 and higher.
- **IBM DB2 for Linux, Unix and Windows 9.8.x, 10.1.x, 10.2.x** - Customers must provide the DB2 JDBC driver(s). The driver can be copied from your DB2 database. Navigate to <DB2-HOME>\java directory and copy db2jcc4.jar and paste it in a temporary folder that you will point to later during the installation.
- **Oracle Database 11g 11.1.x, 11.2.x -** Customers must provide the Oracle JDBC driver(s) which can be downloaded from http://www.oracle.com/technetwork/database/enterprise-edition/jdbc-112010-090769.html.
  The recommended driver file is ojdbc6.jar.

Database Table Space Requirements

Database	Disk Space
Low volume	100 MB

High volume	1 GB +

Java

One of the supported JDK needs to be installed. The appropriate 64-bit Java JDK/SDK must be installed as determined by the server architecture. Java JDK must have the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files installed. Download and follow the instructions distributed with the policy files::

- Sun Java Development Kit 1.7.x or 1.8.x
- IBM Java Developer Kit 7.0.x. You can check and compare the build date of your Java installation by using the command: /usr/java7_64/jre/bin/java -fullversion

For clients, the default minimum JRE is version 1.7.0. If your environment requires a newer Java JRE, the web.xml parameter MinimumJREVersion may be updated.
Java JDK must have the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files installed. Download and follow the instructions distributed with the policy files:

- Oracle JDK policy files: http://www.oracle.com/technetwork/java/javase/downloads/index.html
- IBM Java JDK policy files for 256bit encryption: https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

Java Heap Size

Default Minimum 1024 MB
Default Maximum 4096 MB if a maximum value is specified greater than available RAM, the TIBCO Vault may fail to start.

Browsers Supported

The TIBCO Vault Administrator interface is supported on the following browsers:

- Apple Safari 6.0.x. 7.0.x (On MAC Only)
- Google Chrome 35.x, 36.0.x, 37.0.x
- Microsoft Internet Explorer 9.0.x, 10.0.x, 11.0.x
- Mozilla Firefox 30.0.x, 31.0.x, 32.0.x

Email

Server Support - The TIBCO Vault server is designed to send emails using any email server that supports the SMTP protocol.
Outlook Plug-in Support - When using TIBCO Vault with the Outlook plug-in, one of the follow MAPI email servers is required:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2007

LDAP

Microsoft Active Directory Windows 2008 or 2008 R2, or 2012 may be optionally used for authentication in addition to the default TIBCO Vault database.

Clients

TIBCO Vault supports the following browsers:

- Internet Explorer 9 or above. When using Internet Explorer, you should change the setting for, Check for newer version of stored pages, to be “Automatically” or “Every visit to this page”
- Mozilla Firefox 22.0.x and above
- When using the Java download client, Java JRE 1.7.0 and above is required

TIBCO Vault supports the following Outlook clients or above:

- Outlook 2013 64 and 32-bit
- Outlook 2010 64 and 32-bit

- Outlook 2007 SP3
- Outlook 2003 SP2 - Outlook 2003 reached end of mainstream support effective 4/14/2009. Support for TIBCO Vault on Outlook 2003 may be limited in some circumstances.

Outlook Plug-in Pre-Requisites:

- Microsoft .NET Framework 4.0 or higher installed on the system.
- Visual Studio 2005 Tool for Office SE Runtime (Install provided).
- Microsoft Office 2007 Primary Interop Assemblies (Install provided).
- For Microsoft Outlook 2010, no Primary Interop Assemblies are required.

Network Ports

As with any enterprise application, changes may need to be made to firewalls and other security systems in a production environment. The following tables list default ports for services required and used within TIBCO Vault. Please note that these are the default ports, you will need to check with the appropriate systems administrator to ensure these ports are used in your enterprise.

REQUIRED INBOUND COMMUNICATION:

Service	Default Port	Source	Description
Web Server HTTPS	443	Everyone	Access Server Web Pages

OPTIONAL INBOUND COMMUNICATION:

Service	Default Port	Source	Description
Web Server HTTP	80	Everyone	Redirect to HTTPS
SSH	22	Valid IP's for remote administration	Remote Server administration
SNMP TCP	199	Monitoring Servers	Allows server monitoring using SNMP Polling
SNMP UDP	161	Monitoring Servers	Allows server monitoring using SNMP Polling

REQUIRED OUTBOUND COMMUNICATION:

Service	Default Port	Source	Description
SMTP	25	Email Server	Used to send TIBCO Vault emails

OPTIONAL OUTBOUND COMMUNICATION:

Service	Default Port	Target	Description
DNS	53	DNS Server	DNS Name Lookups
LDAP	389	Active Directory	Allows server to synchronize with AD
LDAPS	636	Active Directory	Allows server to synchronize with AD
NTP	123	NTP Server	Synchronize time with NTP server
SYSLOG UDP	514	Syslog Server	Use centralized logging for server.

DATABASE PORTS:

Database	Default Port
MS SQL Server	1433
Oracle	1521/1522
MySQL	3306
IBM DB2	50000

Minimum Hardware

Platform	Minimum Hardware Requirements	Minimum RAM Requirements
z-Series	Any Hardware supporting z/Linux	8 GB
p-Series	Power Family Processor	8 GB
HP	Itanium processor	8 GB
Linux	x86 processor at 2.5GHz	8 GB
Windows	x86 processor at 2.5GHz	8 GB

Disk Space Recommendation

TIBCO recommends a minimum of 1 GB to install TIBCO Vault and the TIBCO Vault Administrator should perform the following calculations to determine adequate disk space for attachment storage:

- Average size attachment sent across all TIBCO Vault users (both internal and external)
- How many attachments are sent per day
- Desired retention period

Email attachment Disk Space Calculation Example:

- 3 MB avg. attachment size X 50 attachments per day X 30 day retention period = 4500 MB
- 4500 MB /1000 = 4.5 GB
- 4.5 GB plus 20% contingency = 5.4 GB of storage

Either local storage can be used and/or TIBCO Managed File Transfer Platform Server can be configured as a remote server.

Sizing Guidelines

Hardware sizing guidelines are provided in the following sections based on general rules of thumb and previous experience. There are many factors that should be considered to appropriately size required hardware and we have tried to balance the need to provide simple guidance while minimizing complexity. Therefore, these guidelines are not guarantees of actual performance. Every deployment has unique factors that must be considered.

In addition to the above minimum requirements:

- For managing up to 100 concurrent transfers, two or more processor cores at 2.5 GHz or faster
- For managing up to 200 concurrent transfers, four or more processor cores at 2.5 GHz or faster
- For managing more than 200 concurrent transfers, eight or more processor cores at 2.5 GHz or faster
- Two additional processor cores at 2.5 GHz or better for extensive use of encryption or compression.

The default TIBCO Vault maximum database connection parameter value is set during installation to 400. For high volume file transfer environments, increase the parameter above the default of 400. The database maximum connections parameter should match the TIBCO Vault maximum database connection. Please refer to your database manual for information on how to set this parameter.

Installation Procedure

You must be the system Administrator of the operating system to successfully complete the TIBCO Vault Server installation.
Note:

- On Windows 2008, Windows 7, and Vista systems TIBCO recommends the built-in Administrator's account be used for the installation. If you choose to use a Windows domain user's account that has been added to the Administrators group you will need to disable User Account Control (UAC).
- A Java JDK (Software Development Kit) should have been installed before TIBCO Vault was installed. TIBCO Vault installation and configuration requires the *bin* directory of the JDK to be in your PATH. Instructions on how to do this are shown below.
- The TIBCO Vault "install" scripts must be located in the same directory as the "cfcc.jar" file. If you are executing on a UNIX environment, make sure that the "install.sh" and "uninstall.sh" scripts have the "execute" attribute.

Set Environment Variables

Java running on Windows or UNIX

1. Set the JAVA_HOME environment variable. The JDK directory name may be different in your system:

   Windows: **set JAVA_HOME=….\JDK1.8.0_5**
   UNIX: **export JAVA_HOME=…./JDK1.8.0_5**
2. Set the PATH to point to the Java\bin directory:

   Windows: **set PATH=%JAVA_HOME%\bin:%PATH%** Or **set PATH=….\JDK1.8.0_5\bin;%PATH%**

   UNIX: **export PATH=$JAVA_HOME/bin:$PATH** Or **export PATH=…./JDK1.8.0_5/bin:$PATH**

3. Verify that the path was correctly set by issuing the following command:
   Windows and UNIX: **java –version**
   Sample output:
   Java(TM) SE Runtime Environment (build 1.8.0_05-b11)

Note: If you intend to run the application server as a Windows Service you must set the JAVA_HOME environment variable for the System.

Set Unix Permissions

If you are installing TIBCO Vault on one of the supported UNIX platforms and have uploaded the files needed for installing on UNIX the default permissions should be set to the following:

cfcc.jar	-r-- r-- r--	444
EULA.txt	-r-- r-- r--	444
install-config.xml	-r-- r-- r--	444
install.sh	-r-x r-x r-x	555
installer.jar	-r-- r-- r--	444
server.jar	-r-- r-- r--	444
uninstall.sh	-r-x r-x r-x	555

Running the Automated Install

To start the TIBCO Vault automated install, type the following on the command line:

```
install
```

You will see the following:

```
              TIBCO Vault Installer Release 2.0.0
             (supports versions 2.0.0 and higher)

Please note that this install will perform multiple application
server restarts. For this install, press the ENTER key to
accept defaults and continue.

You must read the license agreement before proceeding with the
installation. Press enter to display the agreement.
```

When you press the <Enter> key you will be presented with the End User License Agreement (EULA). Press the <Enter> key as you read through each page to continue to the next page. Once you get to the last page you will be prompted to accept the license agreement. If you do not want to accept the license agreement type “no” and press <Enter> and the installation will end. Once the EULA is accepted the installation will continue:

```
Addenda:

Do you accept the license agreement? Enter yes or no
yes
```

Step 1: This step will first extract the distribution file called cfcc.jar which contains all files necessary for the installation. It will then extract the web server file called server.jar, which contains the embedded TIBCO Vault web server and detect the java environment variable, JAVA_HOME, if it has been set. If you are installing on a UNIX system using IBM java you will also be prompted with the question if FIPS mode should be enabled on the application server. When the server is placed into FIPS mode, TIBCO Vault will only use FIPS certified cryptographic modules when using SSL (HTTPS). If you wish to change your FIPS mode configurations at a later time see section 5 for how to configure FIPS mode manually.

```
Detected Java version:  1.8.0_05
Detected JAVA_HOME environment variable.
Using C:\Program Files\Java\jdk1.8.0_05 as path to JAVA JDK

************************************************************
Step 1  Extracting distribution
Found distribution file c:\VAULT\cfcc.jar
Use C:\VAULT\cfcc.jar as the distribution? y/n [y]:
Extracting distribution file: C:\VAULT\cfcc.jar
............................................................

Distribution extracted successfully!

Installing application server to C:\VAULT\server
............................................................
```

```
.............................

Using C:\VAULT\server as path to the application server
installation.
C:\VAULT\server\conf\Catalina\localhost
```

If the OS was a UNIX system using IBM java you will be asked if you want to run in FIPS mode:

```
Using C:\VAULT\server as path to the application server
installation.

Do you wish to run in FIPS mode? y/n [n]: n
```

Step 2: This step will set up and verify the connection to the database chosen to use for TIBCO Vault. For this sample install, we used Oracle as the database server. When using Oracle you must have the JDBC driver on the system. See the System Requirements section of this manual for more information. (Note: For installations using a MSSQL database that uses Windows Authentication you must add the domain parameter with the domain name to the end of the database URL. To do this, type "n" when prompted with the default statement, "Use database URL:". You will be given the opportunity to enter a new database URL to use. Copy and paste the URL that is contained in the brackets and then add a semicolon and the domain parameter at the end, (i.e., jdbc:jtds:sqlserver://10.1.2.182:1433/VAULT;domain=*DomainName*) and then press the <Enter> key.)

```
Step 2  Verifying database connection
Select database server type:
Enter 1 for MSSQL
Enter 2 for MySQL Enterprise Server or Community Server
Enter 3 for Oracle
Enter 4 for DB2
: 3

Oracle selected as database server type.

Enter the DNS name or IP Address of the database
server...[localhost]:10.97.142.183
Enter the database port number.....................[1521]:
```

```
Enter the database name.....................[VAULT]:orcl
Enter the database UserID...................[vault]:VAULT
Enter the database Password.................[vault]:VAULT
Please confirm password:

Use database URL: [jdbc:oracle:thin:@10.97.142.183:1521:orcl]? y/n
[y] :

Verifying database connection using the following URL:
jdbc:oracle:thin:@10.97.142.183:1521:orcl

The Oracle JDBC driver is not shipped with this product.
The database vender will be able to supply the necessary file(s).
The recommended driver file is ojdbc6.jar.
Please copy the jar file(s) into the C:\VAULT\server\lib
directory.
After the files are copied, press the enter key to continue.

Successfully established connection to the database.

Start to set up pooling parameters
Select database pooling settings. Enter y to use database pooling,
and n for no pooling. [y]:

Input max active connections (positive integer). [400]:
Input max idle pool size (positive integer). [20]:
Input min idle pool size (positive integer). [10]:
Input max wait time to get a connection when there is no available
connection (in minutes). [1]:
Input time between eviction runs to clean up pool (in minutes).
[20]:
Input min evictable idle time before a connection can be removed
from pool (in minutes). [40]:

Database pooling flag: use pooling
Max active connections: 400
Max idle pool size: 20
Min idle pool size: 10
Max wait to get a connection when there is no available
connection: 1 minutes
Time between eviction runs to clean up pool: 20 minutes
Min evictable idle time before a connection can be removed from
pool: 40 minutes

Use these parameters for database connection pooling? y/n [y]:
```

Step 3: Once the database connection has been established in Step 2, Step 3 will generate the TIBCO Vault database tables.

```
Step 3  Configuring the database
Executing database creation utility....
cmd /E:1900 /c setupdb.bat
"jdbc:oracle:thin:@10.97.142.183:1521:orcl" oracle " VAULT" ****
Allocating DBSetup object...
Determining database version....
Installing database...
Updating database...
Updating tables...
…
…
Updating records...
Done updating database.
Successfully installed database:
jdbc:oracle:thin:@10.97.142.183:1521:orcl
Successfully populated DB tables with default information.
adding URIEncoding attribute to http connector
```

If a TIBCO Vault database already exists, then TIBCO Vault will either skip this step or update the tables with the necessary information needed so your database does not get overwritten. Upgrading to a newer version of software using this installation method will not result in lost records or corruption of the existing table structure. When performing a software upgrade, TIBCO recommends that a backup of the database be taken prior to the upgrade. You will see the following:

```
Step 3  Configuring the database
Database is up-to-date.
Executing database creation utility....
cmd /E:1900 /c setupdb.bat
"jdbc:oracle:thin:@10.97.142.183:1521:orcl" oracle VAULT ********
vault

C:\VAULT\distribution\setup>setlocal EnableDelayedExpansion
Allocating DBSetup object...
Determining database version....
Database jdbc:oracle:thin:@10.97.142.183:1521:orcl is up-to-date.
Successfully populated DB tables with default information.
adding URIEncoding attribute to http connector
```

Step 4: This step configures the TIBCO Vault web server for SSL communications. If you do not have a certificate, then the TIBCO Vault install will create a java keystore and a self signed certificate for the server. You can either use a certificate issued by a Certificate Authority (CA) or use a self signed certificate. During the process you will have the opportunity to choose the signature algorithm that will be used to sign the self-signed certificate, the highest strength being SHA512 with RSA and the lowest being SHA1 with DSA. If you are unsure what should be used in your environment choose the default setting of SHA1 with RSA.
Note:

- When asked to, "Enter the DNS name or IP Address of your server", we strongly suggest using a DNS Name. This value is used in the Email URL field defined in the TIBCO Vault System Configuration. The URL will be referenced in emails sent out by TIBCO Vault. Although you can use an IP Address as indicated it is not recommended because if a change to the server's IP address is ever needed in the future, the emails that had been sent out by TIBCO Vault prior to the IP change will no longer be functional.
- Self signed certificates are only practical for testing purposes but do allow you to get up and running quickly while you wait for an external CA to sign a certificate for you.
- Assigning port numbers below 1024 (so-called 'low numbered' ports) can only be bound to by root on UNIX systems.

```
Step 4  Evaluating the application server installation for HTTPS
connectors
Reading the application server configuration file:
C:\VAULT\server\conf\server.xml
Found no pre-existing HTTPS connectors!
Do you have a pre-existing Java Keystore to be used as a server
key for SSL communication? y/n/? [n]:

Creating keystore for SSL communication
Enter the keystore path and
filename..[C:\VAULT\keystore\keystore.jks]:
Directory C:\VAULT\keystore does not exist! Create? y/n [y]:
Enter the keystore password (at least 6 characters)..[changeit]:
```

```
Enter the alias of your private key.....................[vault]:
Enter the DNS Name or IP Address of your
server............:10.97.142.191
Select the signature and key algorithms you wish to use........:
1. SHA1 with RSA
2. SHA256 with RSA
3. SHA384 with RSA
4. SHA512 with RSA
5. SHA1 with DSA
Please enter your selection. [1]: 4
Enter your Company Name.....................[Optional]:TIBCO
Enter your Organizational Unit Name...    ....[Optional]:Web Dpmt
Enter the City where your company is located..[Optional]:Palo Alto
Enter the State where your company is located.[Optional]:CA
Enter the two-letter country code for this unit.[Optional]:US

Keystore filename    : C:\VAULT\keystore\keystore.jks
Keystore password    : ********
Key alias            : vault
Server address       : 10.97.142.191
Signature and key alg: SHA512withRSA
Organization         : TIBCO
Organizational Unit  : Web Debt
Locality             : Palo Alto
State                : CA
Country              : US
Create a keystore with the above information? y/n [y]:

Creating keystore......
C:\Program Files\Java\jdk1.8.0_05\bin\keytool -genkey -keystore
C:\VAULT\keystore\keystore.jks -storepass ******** -keypass
******** -keyalg RSA -sigalg SHA512withRSA -alias vault -keySize
2048 -validity 3650 -dname CN=10.97.142.191, O=TIPCO, OU=Web Dpmt,
L=Palo Alto, ST=CA, C=US

Enter the HTTPS Port to listen for connections… [443]:
```

Step 5: This step will configure the TIBCO Vault components and ports on the application server. This includes the HTTP, AJP, and shutdown request ports. The AJP port is used for forwarding requests from an HTTP server.

```
Step 5  Updating the application server Connector Configuration

Default HTTPS Connector parameters for port 443:
The Default Verbosity Level                          - 2
```

```
The Default Debug Level                                  - 2
The Default Buffer size                                  - 2048
The Default Connection Timeout                           - 60000
The Default DNS Lookup set to                            - true
The Default Max active requests                          - 128
The Default Min Processors                               - 5
The Default Max Processors                               - 100

Accept these parameters? y/n [y]:

Enter the HTTP port to listen for connections... [80] :

Enter the port to listen for shutdown requests... [6005] :

Enter the AJP port... [6009] :
```

Step 6: This step will configure the context root that will be used in the URL. The context name should be set to an alphanumeric name. Using special characters within a context name can cause unpredictable results.

```
Step 6  Evaluating the application server installation for
contexts
Enter the context root for this installation ........[vault]

Reading context configuration file:
C:\VAULT\server\conf\Catalina\localhost\vault.xml
Found no pre-existing Contexts
```

Note: If you are upgrading you will be prompted to backup your present settings as only one instance of vault can exist on the server.

Step 7: This step will extract the vault.war file in order to install the TIBCO Vault application.

```
Step 7  Installing web application
Use C:\VAULT\server\webapps\cfcc as the installation directory?
y/n/? [y]:

Extracting distribution\cfcc.war to C:\VAULT\server\webapps\vault
```

Step 8: This step will verify the context configuration for TIBCO Vault.

```
Step 8  Updating the application server context configuration
```

```
Default Context parameters:
The Default Log File Prefix                    - localhost_cfcc_
The Default Log File Suffix                    - .txt
The Default Log File Timestamp                 - true
The Default Log File Verbosity Level           - 2
The Default Log File Debug Level               - 0

Add a new context with the above parameters? y/n/? [y]:
```

Step 9: This step will update the TIBCO Vault web.xml file with the necessary values to run the Administrator service that controls the TIBCO Vault Administrator web pages. The TIBCO Vault Administration service should only be installed on the internal network.

```
Step 9 Configuring web.xml

Enter the name of the host on which the application will run.
[SystemA]:

Administrator service is used to manage the application.
You should only install this service inside your internal network.
Install this service? y/n? [y]:

Enter a directory to store log files......[c:\VAULT\logs]:
Enter a directory to store temporary files......[c:\VAULT\temp]:

Configure web.xml with the above parameters? y/n [y]:
Starting the application server.................. [OK]
```

Step 10: This step will deploy the TIBCO Vault web service.

```
Step 10 Deploying services
Executing deploy command.
Cmd /E:1900 /c deploy.bat 127.0.0.1 80 admin ****** vault
This may take a few moments......
```

Step 11: This step will generate the SOAP stubs TIBCO Vault will use.

```
Step 11 Generating SOAP Stubs
Executing genstubs command.
Cmd /E:1900 /c genstubs.bat 10.97.142.191 80 admin ****** vault
http
This may take a few moments......
```

Step 12: This step will install the stubs generated for the TIBCO Vault web service in Step 11.

```
Step 12 Installing SOAP Stubs
Executing installstubs command.
Cmd /E:1900 /c installstubs.bat c:\VAULT\server\webapps\vault
This may take a few moments......
```

Step 13: This step will generate the files necessary to show the end-user web pages in various supported languages include English, French, Italian, Portuguese, Spanish and German.

```
Step 13 Generating Multilanguage Support Files
Executing mlxml2properties command.
Cmd /E:1900 /c mlxml2properties.bat c:\VAULT\server\webapps\vault
This may take a few moments......
```

Step 14: This step will digitally sign certain jar files.

```
Step 14 Signing Transfer Applets
Executing signjars command.
Cmd /E:1900 /c signjars.bat c:\VAULT\keystore\keystore.jks *******
cfcc c:\VAULT\server\webapps\vault
This may take a few moments......
```

Step 15: This step is to verify you have installed the required AES encryption policy files needed for TIBCO Vault. If you have not already installed the policy files please refer to the System Requirements section to read about how to obtain the files you need. If your policy files have been installed you will not see the first half of this message.

```
Step 15 Installing AES encryption library
In order to use 256 bit secure keys you must download the JCE
Unlimited Strength Jurisdiction Policy Files from
http://java.sun.com. After downloading, unzip the zip file to
/usr/java/jdk1.8.0_05/jre/lib/security.

Press ENTER to continue.
```

```
Your Java Runtime Environment (JRE) must be upgraded to support
AES encryption. Proceed with the upgrade (recommended)? y/n/? [y]:

Restarting server
Stopping the applicat1on Server..................... [OK]
Starting the applicat1on Server..................... [OK]

Installation completed! Details are in the install.log file.
```

The TIBCO Vault automated install is complete.

If you are installing TIBCO Vault on a Windows system a Java window labeled TIBCO Vault Server will display during the installation process. This window must be kept opened in order for the TIBCO Vault server to continue running. Closing the TIBCO Vault Server window will shutdown the web application.

You may stop and start the Vault Server by running the **startup** and **shutdown** scripts for the appropriate system in the server directory at: <TIBCO Vault_Install>/server/bin

Once TIBCO Vault is installed successfully, it is time to access the TIBCO Vault Administrator web pages.
The TIBCO Vault is accessed using one of the following URLs:

https://[DNS_HostName]:[httpsPort]/[context]/control?view=view/admin/start.jsp
or
https://[DNS_HostName]:[httpsPort]/admin

Note: If the default context was not used during installation, the redirector file for this shortcut as well as others mentioned later in this manual will need to be updated to redirect to the non standard context. Follow the instructions below to make these changes:
The redirection files can be found in the <TIBCO Vault_Install>\server\webapps\ROOT directory. Use a text editor to open and change the “vault” context in these files to the new context

chosen during the install. Once your changes have been made save and close the files.

When you are prompted for a userid/password you must log in with the Administrator credentials of **admin/changeit** (the password is case sensitive).

Setting Java Heap Size (Optional)

By default, the web server's Java Heap memory size is set to 512 MB minimum and 1024 MB maximum size. Ensure that your server meets the required amount of physical memory before installing TIBCO Vault.

The memory heap size can be increased after installing TIBCO Vault using the following methods:

For the embedded Web Server

1. Navigate to the following directory based on your operating system:

   Windows File Name: <Vault_install>\server\bin\setenv.bat
   Linux File Name: <Vault_install>/server/bin/setenv.sh

2. Open the file with a text editor to and edit the following variable settings:

   @echo off
   SET CATALINA_OPTS=-Xms512m -Xmx1024m
   SET TITLE=TIBCO Vault Server
   To change the minimum heap size value, alter the "–Xms" parameter.
   To change the maximum heap size value, alter the "–Xmx" parameter.

Configuring Auto Start at Boot-up

By default the application server is not configured to automatically start on boot-up. This section describes how to setup an automatic start for

the TIBCO Vault embedded application server on a Windows or UNIX/Linux system.

For a Windows Service

First check the JAVA_HOME System environment variable has been configured on your server. To set the variable open your System Properties window and click on the Advanced Tab. Click on the button with the name *Environment Variables* on it. In the bottom window labeled, System variables, search for the JAVA_HOME variable. If you do not see it in the list you must add the JAVA_HOME variable pointing to your Java's jdk file. For example: C:\Program Files\Java\jdk1.6.0_29.

Note: If you created a new variable you must restart the system before the new variable will be recognized.

Next navigate to the <TIBCO Vault_Install>\server\bin directory and stop your present TIBCO Vault application using the shutdown command. Once the server has stopped run the following install command from the same directory:

service install

You will be prompted to choose which processor you are currently running with as seen in the example below:

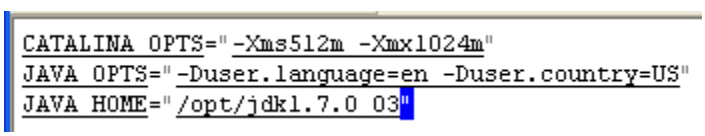
```
C:\VAULT\server\bin>service install

This script will create or remove the TIBCO Vault Windows server.
Please select your processor type

1.      32 bit Intel            <x86-32>
2.      64 bit Intel/AMD        <x86-64>
3.      64 bit Intel Itanium    <IA-64>
4.      Exit script

Type selection: 2
Installing the service 'TIBCO VaultServer' ...
Using CATALINA_HOME:    "C:\VAULT\server"
Using CATALINA_BASE:    "C:\VAULT\server"
Using JAVA_HOME:        "C:\Program Files\Java\jdk1.6.0_29"
Using JVM:              "%JAVA_HOME%\jre\bin\server\jvm.dll"
The service 'TIBCO VaultServer' has been installed.
```

Once the script has completed running open your Services by navigating to Start > Administrative Tools > Services. There should be a service listing called **TIBCO Vault Server**.

For UNIX/Linux Systems

There are a number of methods that different UNIX/Linux operating systems use to automatically start processes at boot time. This example has been developed specifically for the Red Hat Linux Enterprise operating system, but has been tested successfully on many other UNIX and Linux distributions. The instructions for setting auto start on Red Hat Linux are:

In order to have the TIBCO Vault automatically start on boot-up, first add the JAVA_HOME variable to the <TIBCO Vault_Install>/server/bin/setenv.sh file:



Then add the startup.sh shell script to the /etc/rc.local file.

For example: /opt/TIBCO Vault/server/bin/startup.sh

Remove Windows Auto Start Settings

Should you want to remove the auto start feature stop the TIBCO Vault Server service and navigate to the <Vault_Install>\server\bin directory and run the following command:

service remove

The service will be removed.

Uninstall TIBCO Vault

To uninstall TIBCO Vault you would use the **uninstall.bat** program for Windows installations or **uninstall.sh** program for UNIX installations located in your <Vault_Install> directory.

Note: If TIBCO Vault has been installed as a Windows service it should be removed before running the uninstall.bat. Please remove the TIBCO Vault service by following the instructions from the Romove Windows Auto Start section seen above.

From the command line run the following command on either Windows or UNIX:

uninstall

In the example below we ran the **uninstall.bat** on an TIBCO Vault installation:

```
uninstall

Please note that this uninstall will perform multiple App Server
restarts.
For this uninstall, press the ENTER key to accept defaults and
continue.

Stopping the application
server.................................[OK]

Uninstalling the application server HTTPS connector..........

Uninstalling context......
Deleted distribution directory.

The uninstall has completed! Details are in the uninstall.log
file.
```

Your TIBCO Vault uninstall is complete.

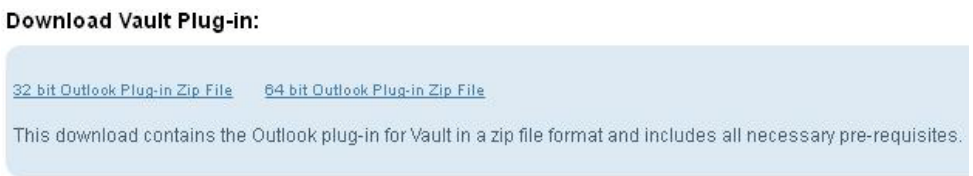
As mentioned TIBCO Vault has two interfaces the browser interface and the Outlook Plug-in. In this section we will discuss the TIBCO Vault Outlook Plug-in. This plug-in allows the end user to utilize all TIBCO Vault's functions from the popular Microsoft Outlook Application. See the System Requirements section of this manual for more information on what is required for installing the TIBCO Vault Plug-in.

TIBCO Vault Outlook Plug-in Install

To download the Outlook Plug-in to be installed on a Desktop either the end user or the Administrator would use one of the following URLs:

https://[DNS_HostName]:[httpsPort]/[context]/control?view=am/start.jsp&action=config.am

You will see a page similar to the one below:

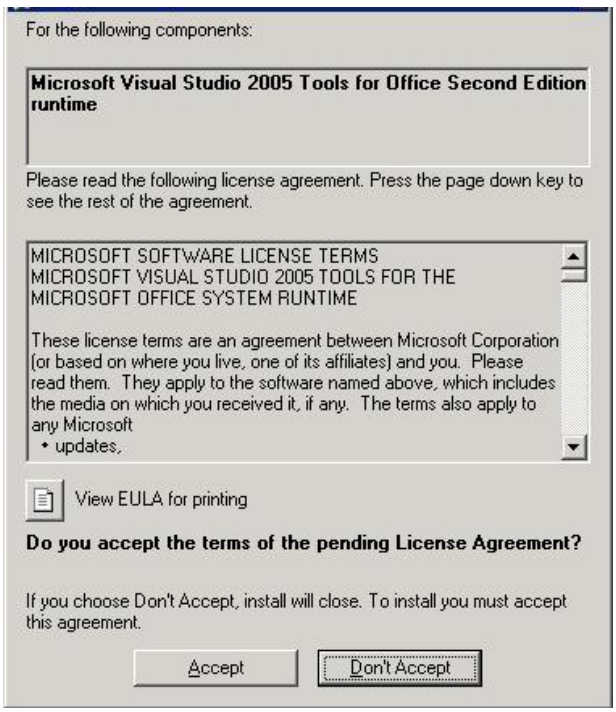


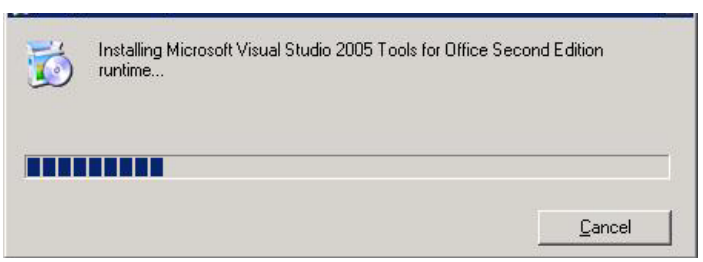
From the screen shot above the end user can download the installation as an executable or in zip file format. The executable file can be used if all the pre-requisites are installed already. Otherwise the zip file format should be downloaded.

Click on the link to start the download.

Note: For our example we will be using the **setup.exe** which is contained in the TIBCO Vault Outlook Plug-in Zip File to install the plug-in product on a system for the first time.

Running the install using the **setup.exe** is recommended because it will install everything the product needs except for the Microsoft .NET Framework v4.0 or higher. The first component it will look for is the Microsoft Visual Studio 2005 Tools for Office runtime. If this is not found you will be prompted to install it as seen below:





A reboot of the system may be required at this point.

Once the Microsoft runtime library in installed and the system rebooted double click on the **setup.exe** file again. TIBCO Vault will then check if the 2007 Primary Interop Assemblies program is installed. If not it will install the program for you. These components are needed for the TIBCO Vault Outlook plug-in interoperability between its .NET managed code and Microsoft Office COM libraries. Once this install is complete double click on **setup.exe** file again in order to install the TIBCO Vault Outlook Plug-in.

For more information on how to use the Outlook Plug-in please see the *TIBCO Vault v1.1.0 User Guide*.

TIBCO Vault Outlook Plug-in Silent Install

The TIBCO Vault Outlook Plug-in can be deployed throughout your environment through a silent install. Below are general instructions to follow when using Microsoft System Management Server (SMS):

Note: Every computer receiving the TIBCO Vault Outlook Plug-in must meet the Pre-Requisites as defined in this manual in section 2.

If using collections that were previously defined, make sure to update the collection before deployment.

1) Define your distribution points for the package.
2) Create a new collection or use a predefined collection to specify clients which will receive the TIBCO Vault install.
3) Gather all source files, setup routines, scripts, and so on, needed for the package.
4) Create the Configuration Manager package.
5) Define the TIBCO Vault program for the package.
6) On the General program configuration page, define the “Command line” parameter AMURL for the TIBCO VaultOutlookPlugIn.msi. (See example below)
7) Distribute the package to the distribution points.
8) Advertise the programs to one or more collections.
9) Execute the advertised program on the client.

Example of SMS Command Line with options for TIBCO Vault Outlook Plug-in program deployment:

TIBCO VaultOutlookPlugIn.msi /q AMURL=https://[host]:[port]/[context]

For more details on using SMS for silent installations, please refer to Microsoft’s online SMS Guides:

http://technet.microsoft.com/en-us/library/bb735860.aspx

Hiding the Outlook TIBCO Vault Send Button

For Outlook 2003 Clients, the TIBCO Vault Send button can be hidden from the Outlook TIBCO Vault toolbar by adding the following registry key value:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TIBCO\TIBCO
Vault\HideSendButton
```

Set to DWORD 1 TIBCO Vault Outlook

Upgrade

This chapter will assist users upgrading from previous versions of TIBCO Vault as well as instruct the Administrator what is needed when upgrading the Java JDK on Windows. Some steps in the upgrading process will differ, depending on the version of the former TIBCO Vault you have installed presently.

Topics

TIBCO Vault Upgrade

Upgrade from v1.0.0, v1.0.1, and v1.1.1

For those that are upgrading from release level 1.0.0, 1.0.1, and v1.1.1 a new installation must be done to upgrade your version of Vault.

Step 1) Stop the application server.

Step 2) Backup your <Vault_Install> installation directory.

Step 3) Backup your Vault database.

Step 4) If you are running on a Windows platform and have installed the Auto Start program you will need to remove the service from the old installation directory and reinstall it from the new installation directory. See Removing Auto Start for instructions.

Step 5) During the installation you will be asked if you have a pre-existing keystore. If you want to use this pre-existing keystore make note of the full path and be prepared to enter the private key password.

Step 6) You will need to download the supported database driver(s) needed as per the instructions found in the System Requirements section of this manual.

Step 7) Create a new directory and copy all the v2.0.0 files into that new directory or copy and replace all the v2.0.0 files into the existing installation directory. Follow the Running Automated Install section of this manual.

Step 8) If you are running on a Windows platform you can install the Auto Start program at this time from the new installation directory. See Configure Auto Start at Bootup for instructions.

Java JDK Upgrade

When upgrading the Java JDK that is being used by Vault you will need to update a few items before the Vault will start to use the new Java JDK.

1. If Vault is running on a Windows system and is running as a service, stop the Vault service.
2. Go to <VAULT_Install>\server\bin directory and run the following command and answer the question(s) to uninstall the service:

   service remove

3. Update the JAVA_HOME environment variable on the system to point to the new JDK directory. I verify the system is pointing to the new Java JDK run the following command to verify the version:

   java –version

4. Update the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. For more details see the pre-requisites for Java of this manual.
5. From the <VAULT_Install>\distribution\crypto directory copy files **bcprov-jdk15on-147.jar** and **bcprov-ext-jdk15on-147.jar** to the following <JAVA_HOME>\jre\lib director.
6. From the <VAULT_Install>\distribution\crypto directory copy file **bcpg-jdk15on-147.jar** to < Vault_Install>\server\webapps\<context>\WEB-INF\lib directory.
7. Backup the file **java.security** found in the following directory <JAVA_HOME>\jre\lib\security.
8. Open the file **java.security** using notepad on Windows or vi editor on UNIX. Scroll down until you see the comment

"# List of providers and their preference orders (see above)". Add the following security provider if you do not see it in the list at position 3 and reorder the other security providers as necessary:

security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider

9. If Vault is installed on a Windows system you can now go to <VAULT_Install>\server\bin directory and run the following command and answer the question(s) to install Vault to run as a service:

   service install

10. Start Vault Service.

Customizing TIBCO Vault

This section will guide you through the required configuration steps to customize your TIBCO Vault Installation.

Topics

- *Administrator Browser Interface*
- *End User Browser Interface*
- *Email Templates*

Web Pages And Email Templates

Administrator Browser Interface

TIBCO Vault Administrator logo (upper left corner)

- Path and File Name: \vault\public\images\vault\ic-header-logo.png
- Height 18 px
- Width 154 px

TIBCO logo (bottom left)

- Path and File Name: \vault\images\tibco-logo-117-24.jpg
- Height 24 px
- Width 117 px

End User Browser Interface

TIBCO Vault Logo (upper left corner)

- Path and File Name: \vault\public\images\vault\ic-header-logo.png
- Height 18 px
- Width 154 px

Header Background Image

- Path and File Name: \vault\public\images\am/bg_header.jpg
- Height 65 px
- Width 623 px

Header Background Image

- Path and File Name: \vault\public\images\am\tibco_logo.png
- Height 30 px
- Width 95 px

Login Web Pages

Used for the following Login web pages:

Administrator

Browser Client

TIBCO Login Vault Logo (upper left corner)

- Path and File Name: \vault\amlogin\images\ic-header-logo.png
- Height 18 px
- Width 154 px

TIBCO Logo (bottom left corner)

- Path and File Name: \vault\amlogin\images\ic-footer-logo.png
- Height 14 px
- Width 64 px

Header Background Image

- Path and File Name: \vault\amlogin\images\bkg_header.png
- Height 73 px

- Width 1200 px

Background Image (smiling male)

- Path and File Name: \vault\amlogin\images\img-hero.jpg
- Height 602 px
- Width 1200 px

Please follow these steps for customizing your TIBCO Vault logos:

1. Locate the directory where the logos are stored
2. Rename the logo that is being replaced by adding .OLD after .GIF (e.g., logo.gif.old)
3. Copy your new logos into the directory and make sure the file names match the original file names in the directory.
4. Refresh your browser.

Note: Your new logos should be the same size as the TIBCO Vault logos being replaced.

Email Templates

TIBCO Vault uses a standard set of templates for outgoing emails. These files are in XML format and can be edited using an XML editor. The files can be found in the following directory:

vault\email-template

List of the templates that can be edited with their file names:

1) Alert Notifications:
email-alert-notification-template.xml

2) Default template sent on every TIBCO Vault email:
Vault-file-available-template.xml

3) Download Notification Template:
Vault-file-downloaded-template.xml

4) Forgot User Name Request:
Vault-forgot-username-template.xml

5) Disabled Email Notification:
Vault-recall-message-template.xml

6) Self Registration Success:
Vault-register-success-template.xml

7) Self Registration Request:
Vault-register-user-template.xml

8) Reset Password Request:
Vault-reset-password-template.xml

9) Reset User Name and Self Registration Unsuccessful:
Vault-reset-username-register-failure-template.xml

Please follow these steps for customizing your TIBCO Vault email templates:

Step 1) Locate the \vault\email-template\ directory where the templates are stored. Rename the template that is being replaced by adding .OLD after .XML (e.g., email-alert-notification-template.xml.old)

Step 2) Copy your new template into the directory and make sure the file name matches the original file name in the directory.

Step 3) Any new emails sent from the server will use the new email template.

Multi-Language Support

By default the TIBCO Vault Interface's support only the English language at this time.

Appendix A: Setting Cipher Algorithms

This section contains instructions on how to configure TIBCO Vault Server to only accept connections from clients using specific high strength cipher algorithms.

Topics

- *HTTP SSL Ciphers*

HTTP SSL Ciphers

For an increased level of HTTP SSL security in TIBCO Vault Server, running the server in FIPS mode is recommended. If you do not have your TIBCO Vault Server running in FIPS mode however, and higher HTTP SSL cipher strengths are required for client connections, you can edit the following TIBCO Vault configuration file to enforce certain SSL ciphers.

```
<TIBCO Vault_Install>/server/conf/server.xml
```

Within this file is a default HTTP connector that contains the ciphers default value of “All” as seen below:

```
<Connector SSLEnabled="true" URIEncoding="UTF-8"
acceptCount="128" clientAuth="false" compression="off"
connectionLinger="-1" connectionTimeout="60000"
disableUploadTimeout="true" enableLookups="true"
keystoreFile="C:\VAULT\keystore\keystore.jks"
keystorePass="changeit" keystoreType="JKS"
maxKeepAliveRequests="100" maxThreads="150" port="443"
protocol="org.apache.coyote.http11.Http11Protocol"
proxyPort="0" redirectPort="-1" scheme="https"
secure="true" socket.txBufSize="65536"
sslEnabledProtocols="TLSv1, TLSv1.1, TLSv1.2"
ciphers="All" sslProtocol="TLS" tcpNoDelay="true"/>
```

The list of available ciphers can be found by navigating to the TIBCO Vault Diagnostics web page and expanding the window for the TIBCO Vault Server clients will be connecting to.

Below is an example that will force client connections to maintain cipher strengths of 128bit or greater. *Note: The ciphers in this example are from Oracle Java 8 update 5*:

```
ciphers="SSL_RSA_WITH_RC4_128_MD5,
SSL_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA,
```

```
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
```

Below is another example that will force client connections to maintain cipher strengths of 256bit or greater *Note: Only certain browsers will support 256bit cipher strength. The ciphers in this example are from Oracle Java 8 update 5:*

```
ciphers="TLS_RSA_WITH_AES_256_CBC_SHA"
```

We have taken the example above and placed it in our default Connector to show how this would be added:

```
<Connector SSLEnabled="true" acceptCount="128"
bufferSize="2048" clientAuth="false" compression="off"
connectionLinger="-1" connectionTimeout="60000"
debug="2" disableUploadTimeout="true"
enableLookups="true"
keystoreFile="C:\VAULT\keystore\keystore.jks"
keystorePass="changeit" keystoreType="JKS"
maxKeepAliveRequests="100" maxProcessors="100"
maxThreads="150" minProcessors="5" port="443"
protocol="org.apache.coyote.http11.Http11Protocol"
proxyPort="0" redirectPort="-1" scheme="https"
secure="true" sslProtocol="TLS"
ciphers="TLS_RSA_WITH_AES_256_CBC_SHA" tcpNoDelay="true"
useURIValidationHack="true"/>
```

Once you have saved your changes, you must restart the application server.

TIBCO Vault Worksheet

This section contains a worksheet that is designed to allow you to have one convenient location to collect information that will be used throughout the installation and configuration of the TIBCO Vault Server.

Topics

Install Worksheet

JDK Information

1. Which version of Java JDK is installed on the server

_____

2. Do you have variables “JAVA_HOME” and “PATH” set:

_____

3. Have you downloaded and installed the Java AES encryption policy files: _____

Database Information

4. What is the IP Name/Address and port number for the TIBCO Vault database: _____

5. What is the name of the database to be used for TIBCO Vault:

_____

6. What is the id and password for the database:

_____

Java Keystore Information

(Only needed if TIBCO Vault self-signed certificate is not being used)

7. What is the path and file name of your java keystore:

_____

8. What is your keystore password: _____

9. What is the alias for the private key: _____

TIBCO Vault Application Information

10. What is the IP Name/Address of the server where TIBCO Vault will is being installed? _____

11. What context root do you want to use (default is vault):

_____

12. In what directory should log files be kept (defaults to install directory): _____

LDAP Information

(Only needed if using LDAP for authentication)

13. LDAP server type: _____

14. DNS or IP Address of the LDAP server:

_____

15. What is the LDAP port number: _____

16. What is the LDAP Administrator DN:

_____

17. What is the password for the User DN:

_____

Data Store Information

18. Where will attachments for TIBCO Vault be stored:

    Local Hard Disk ___

    TIBCO MFT Platform Server ___

    Other Storage Device ___.

19. Path and folder name where active TIBCO Vault attachments will be stored: _____

Email Server Information

20. What is the IP Name/Address and port of the email server being used by TIBCO Vault: _____

21. Has the right to relay SMTP emails been granted to the TIBCO Vault server: _____