



# **TIBCO ActiveMatrix® Service Grid**

## **Installation and Configuration**

*Software Release 3.4.0*

*April 2019*

*Document Updated: December 2019*

## 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 (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.

ANY SOFTWARE ITEM IDENTIFIED AS THIRD PARTY LIBRARY IS AVAILABLE UNDER SEPARATE SOFTWARE LICENSE TERMS AND IS NOT PART OF A TIBCO PRODUCT. AS SUCH, THESE SOFTWARE ITEMS ARE NOT COVERED BY THE TERMS OF YOUR AGREEMENT WITH TIBCO, INCLUDING ANY TERMS CONCERNING SUPPORT, MAINTENANCE, WARRANTIES, AND INDEMNITIES. DOWNLOAD AND USE OF THESE ITEMS IS SOLELY AT YOUR OWN DISCRETION AND SUBJECT TO THE LICENSE TERMS APPLICABLE TO THEM. BY PROCEEDING TO DOWNLOAD, INSTALL OR USE ANY OF THESE ITEMS, YOU ACKNOWLEDGE THE FOREGOING DISTINCTIONS BETWEEN THESE ITEMS AND TIBCO PRODUCTS.

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, TIBCO O logo, TIB, Information Bus, ActiveMatrix, Business Studio, Enterprise Message Service, Hawk, and Rendezvous are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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. Please 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 © 2010-2019. TIBCO Software Inc. All Rights Reserved.

# Contents

<b>Figures .....</b>	<b>12</b>
<b>TIBCO Documentation and Support Services .....</b>	<b>13</b>
<b>Setting Up an Enterprise .....</b>	<b>15</b>
<b>Installation Overview .....</b>	<b>17</b>
<b>Installation Requirements .....</b>	<b>18</b>
Installation Account Requirements .....	18
Hardware Requirements .....	18
Software Requirements .....	19
Database Requirements for SPM .....	22
Installation Environment .....	22
Installation Profiles .....	23
<b>Pre-installation .....</b>	<b>25</b>
Configuring External Databases .....	25
Database Privileges Needed for Automatic Schema Creation .....	25
Database Privileges Needed for Manual Schema Creation .....	26
Configuring Ant .....	27
Configuring AIX Platforms .....	28
Configuring the Environment Settings for AIX Platforms Versions .....	28
Configuring the Maximum Number of Open Files on Linux Platforms .....	29
Downloading Software Assemblies if No Internet Access is Available .....	29
Installation and Configuration Checklist .....	30
<b>Installing TIBCO ActiveMatrix Service Grid .....</b>	<b>32</b>
Installing in GUI Mode .....	32
Installing in Console Mode .....	34
Installing in Silent Mode .....	34
Moving an Installation to a Destination Machine .....	35
Verifying Installation .....	35
TIBCO_HOME Files and Directories .....	36
<b>Configuration .....</b>	<b>40</b>
Configuration Setup and Overview .....	40
Networking .....	40
Default Ports .....	40
Secure Communication Channels .....	42
Keystores .....	44
Trust Stores .....	45
Creating a Trust Store Keystore .....	45

Configuring a Trust Store .....	45
IPv6 Support .....	46
TIBCO Configuration Tool Requirements .....	47
Enterprise Messaging Server Requirements .....	48
SSL Requirements .....	48
Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users .....	49
Determining Whether an Enterprise Needs a Messaging Bus .....	50
Running TIBCO Configuration Tool .....	53
Running TIBCO Configuration Tool in GUI Mode .....	53
Running TIBCO Configuration Tool in Console Mode .....	55
Running TIBCO Configuration Tool in Silent Mode .....	56
Using TIBCO Configuration Tool Scripts and Property Files .....	57
Saving a TIBCO Configuration Tool Configuration .....	59
Reusing a TIBCO Configuration Tool Configuration .....	59
Configure Third-Party Driver Properties .....	60
Create TIBCO Host Instance Properties .....	61
Create ActiveMatrix Administrator Server Properties .....	62
Modifying Scripts from Earlier Releases .....	63
Configuration Tool Wizards and Screens .....	64
Create Express Developer Environment .....	64
Administrator Server Configuration Details .....	65
Administrator Server Notification and Messaging Bus Server .....	65
Summary .....	66
Create TIBCO ActiveMatrix Administrator Server .....	67
Administrator Server Configuration Details .....	71
Administrator Server TIBCO Host Configuration .....	72
Administrator Server Connection Settings .....	73
Administrator Server Internal HTTP Port .....	74
Administrator Server Notification and Messaging Bus Server .....	74
Administrator Server Enterprise Message Service Connection Factory .....	76
Administrator Server Database Details .....	76
Administrator Server Authentication Realm .....	78
Administrator Server Database Authentication Realm .....	79
Administrator Server LDAP Authentication Realm .....	81
Administrator Server TIBCO Credential Server Details .....	84
Administrator Server TIBCO Credential Server Keystore .....	85
Administrator Server Logging Notification Server .....	85
Administrator Server Log Service Database .....	87
Administrator Server Payload Service Database .....	89

Summary .....	91
Create TIBCO ActiveMatrix Policy Director Governance Administrator Server .....	92
TIBCO ActiveMatrix Policy Director Governance Administrator Server Selection .....	94
Administrator Server Configuration Details .....	95
Administrator Server TIBCO Host Configuration .....	96
Administrator Server Connection Settings .....	97
Administrator Server Connection Details .....	98
Administrator Server Internal HTTP Port .....	99
Administrator Server Notification and Messaging Bus Server .....	99
Administrator Server Enterprise Message Service Connection Factory .....	101
Administrator Server Database Details .....	101
Administrator Server Authentication Realm .....	103
Administrator Server Database Authentication Realm .....	104
Administrator Server LDAP Authentication Realm .....	106
Administrator Server TIBCO Credential Server Details .....	109
Administrator Server TIBCO Credential Server Keystore .....	110
Administrator Server Log Service Database .....	110
Administrator Server Payload Service Database .....	112
Proxy Management Services Configuration .....	115
Summary .....	115
Create TIBCO ActiveMatrix Policy Director Governance Proxy Host .....	116
TIBCO ActiveMatrix Policy Director Governance Proxy Host Creation Wizard .....	116
TIBCO Host Selection .....	116
TIBCO Host Instance .....	117
TIBCO Host Instance Notification Server .....	117
TIBCO Host Instance Administrator Server .....	118
Proxy Node Configuration .....	120
TIBCO ActiveMatrix Policy Director Governance Proxy Host Configuration Summary .....	120
Create TIBCO Host Instance .....	121
TIBCO Host Instance .....	121
TIBCO Host Instance Notification Server .....	122
TIBCO Host Instance Administrator Server .....	123
Summary .....	124
Configure Third-Party Driver .....	125
Third-Party Driver Details .....	125
Third-Party Driver JAR Folder .....	127
Edit ActiveMatrix Administrator Server Configuration .....	127
Edit Administrator Server Configuration .....	127
Administrator Server Connection Settings .....	128

Edit Administrator Server Database Details .....	129
Making Planned Database Configuration Changes .....	132
Edit Administrator Server Authentication Realm .....	132
Edit Server LDAP Authentication Realm .....	134
Summary .....	136
Replicate TIBCO ActiveMatrix Administrator Server .....	136
Configuring ActiveMatrix Policy Director Governance on Replicated Administrator Server .....	139
Remote Administrator Server Details .....	139
Create Replicated Instance Validation Info .....	140
Administrator Server Configuration Details .....	141
Administrator Server TIBCO Host Configuration .....	141
Administrator Server Connection Settings .....	142
Administrator Server Notification and Messaging Bus Server .....	142
Administration Server Database Details .....	144
Administrator Server Database Authentication Realm Details .....	145
Administrator Server Configuration LDAP Authentication Realm .....	145
Administrator Server Configuration Summary .....	145
Deleting an Administrator Server .....	145
Upgrade or Downgrade TIBCO ActiveMatrix .....	146
Upgrade or Downgrade .....	146
Upgrade Options .....	147
Upgrade Selection .....	147
Validate .....	147
Upgrade Summary .....	148
Downgrade Options .....	149
Downgrade Selection .....	149
ActiveMatrix Administrator Server .....	149
Downgrade Summary .....	149
Update JRE used by TIBCO ActiveMatrix .....	150
Select JRE Home .....	150
Summary .....	150
Configure TIBCO Service Performance Manager .....	151
TIBCO Service Performance Manager Configuration: Database Configuration .....	151
JMS Configuration .....	153
Threadpool Configuration .....	154
Server Configuration .....	155
Storage and Recovery Configuration .....	157
Action Configuration .....	158
Handle Configuration File .....	160

Summary Configuration .....	161
Generate TIBCO Service Performance Manager Database Schema .....	161
Summary Configuration .....	162
Configure TIBCO Service Performance Manager Dashboard .....	162
Generate Database Configuration .....	162
Database Configuration .....	162
JMS Configuration .....	163
Threadpool Configuration .....	164
Server Configuration .....	164
Storage And Recovery Configuration .....	164
Action Configuration .....	164
Handle Configuration File .....	165
Client API JMS Configuration .....	165
Client API Configuration .....	166
Dashboard Server Configuration .....	167
Dashboard Server Security Configuration .....	168
Dashboard Server Authentication LDAP Configuration .....	168
Tomcat Server Configuration .....	169
Dashboard Server Authentication File Configuration .....	170
Summary Configuration .....	170
DDL Script Generator .....	170
Overview of the DDL Script Generator Utility .....	170
Creating the Database Schema .....	171
Cleaning up the Database Schema .....	171
Database Models .....	172
DDLGeneratorTask .....	172
Configuring TIBCO Service Performance Manager Components .....	174
Setting EMS_HOME .....	175
Creating EMS Queues and Factories .....	177
Setting Properties for the SPM Dashboard .....	178
Configuring the SPM Dashboard Server to use the SPM Server .....	178
Configuring TIBCO Service Performance Manager Dashboard Server .....	178
Configuring the TIBCO Service Performance Manager Server .....	179
Generating the Database Schema and Starting the Database .....	180
Configuring TIBCO Service Performance Manager Service Probe .....	180
Service Probe Installation Prerequisites .....	182
Enabling the Service Probe on TIBCO ActiveMatrix Nodes .....	182
Enabling the Service Probe Using TIBCO ActiveMatrix Administrator UI .....	182
Enabling the Service Probe Using TIBCO ActiveMatrix Administrator CLI .....	183



Disabling the Service Probe on TIBCO ActiveMatrix Nodes .....	184
Disabling the Service Probe Using TIBCO ActiveMatrix Administrator UI .....	184
Disabling the Service Probe Using TIBCO ActiveMatrix Administrator CLI .....	184
Client Properties of TIBCO Service Performance Manager .....	184
Changing the Heap Size of the Server .....	189
Logging Configuration .....	190
SPM Server Logging Configuration .....	190
SPM Dashboard Logging Configuration .....	190
SPM Example Logging Configuration .....	190
<b>Using the Service Performance Manager Components .....</b>	<b>191</b>
Starting the TIBCO SPM Server .....	191
Starting the TIBCO SPM Dashboard .....	191
Samples .....	192
Running the Client API Application Example .....	192
Client Properties .....	192
Overriding the Default Property Values .....	194
Deployment Scenarios .....	194
TIBCO Enterprise Message Service Server Deployment .....	195
TIBCO Service Performance Manager Server Deployment .....	195
Improving the Performance .....	196
Data Retention Policies .....	197
<b>Using TIBCO Business Studio .....</b>	<b>199</b>
<b>Upgrade and Downgrade .....</b>	<b>202</b>
Prerequisites for Upgrading or Downgrading .....	202
Upgrade .....	204
Upgrading Runtime Hosts and Nodes .....	206
Post Upgrade Actions .....	207
Creating and Installing Resource Template, Resource Instance required for Service Health Check .....	208
Updating ActiveMatrix Administrator .....	208
Upgrading REST Binding Type .....	209
Upgrading TIBCO Service Performance Manager .....	210
Upgrading TIBCO ActiveMatrix Policy Director Governance .....	211
Supported ActiveMatrix Policy Director Governance Upgrade Scenarios .....	211
Upgrading TIBCO ActiveMatrix Policy Director Governance Installation in TIBCO ActiveMatrix Service Grid 3.3.x .....	212
Upgrading TIBCO ActiveMatrix Policy Director Governance Installation on TIBCO ActiveMatrix Service Grid 3.2.x .....	212
Verifying the Upgrade .....	213
Uninstalling MCR Dashboard Application .....	213

Downgrade .....	214
Downgrading Runtime Hosts and Nodes .....	215
Updating ActiveMatrix Administrator .....	215
Downgrading REST Binding Type .....	216
Verifying the Downgrade .....	217
Using TIBCO Configuration Tool (TCT) to Upgrade or Downgrade .....	217
Diagnostic Tests .....	217
Tests That Are Common to Upgrade and Downgrade .....	218
Additional Tests for Downgrade .....	218
Using GUI Mode .....	219
Using Console Mode .....	219
Using Silent Mode .....	222
Using Scripts .....	223
Upgrading and Downgrading: An Example .....	226
Instance Details .....	227
Upgrading Using TCT Wizard .....	227
Upgrading the ActiveMatrix Administrator Instance .....	227
Upgrading Runtime Hosts .....	233
Verifying Upgrade .....	234
Analyzing the Upgrade Logs .....	237
Start and Stop Action Logs .....	237
Upgrade Action Logs .....	237
Post Upgrade Action Logs .....	238
SystemNode Upgrade Logs .....	239
Downgrading Using TCT Wizard .....	241
Downgrading Runtime Hosts .....	241
Downgrading the ActiveMatrix Administrator Instance .....	245
Verifying Downgrade .....	246
Analyzing the Downgrade Logs .....	248
Start and Stop Action Logs .....	249
Downgrade Action Logs .....	249
SystemNode Downgrade Logs .....	250
Special Case Scenario on Handling REST BT after a Downgrade .....	252
Uninstalling TIBCO ActiveMatrix Service Grid in the GUI Mode .....	253
Deploying REST BT System and User Applications .....	253
<b>Host Manager .....</b>	<b>255</b>
Patch Commands .....	255
describeAvailablePatches .....	255
describeAppliedPatches .....	256

applyPatch .....	256
revertPatch .....	258
Engineering Build Commands .....	260
applyEB .....	260
revertEB .....	262
Host and Node Commands .....	264
startAllHosts .....	264
startAllNodes .....	266
stopAllHosts .....	266
stopAllNodes .....	267
updateManifest .....	268
describeHostUpgradeHistory .....	268
updateWindowsServices .....	269
Miscellaneous Commands .....	270
Common Arguments .....	270
clearLog .....	272
interactive .....	272
intro .....	273
version .....	273
viewLog .....	273
installInfo .....	273
<b>Updating JRE Version .....</b>	<b>276</b>
Approach .....	276
Properties Updated in CLASSPATH .tra Files .....	277
Invoking the Tool .....	277
Help Commands .....	278
Modes of Operation .....	279
Commands .....	279
Discover Mode .....	280
Update Mode .....	281
Reverting to the Previous Version of the JRE .....	283
Backup of Files .....	283
Logging .....	284
<b>Troubleshooting .....</b>	<b>285</b>
<b>Uninstallation .....</b>	<b>292</b>
Prerequisites for Uninstalling .....	292
Uninstalling in GUI Mode .....	292
Uninstalling in Console Mode .....	293

# Figures

---

Default Ports .....	41
Communication Channels .....	42
Messaging Bus Required - Application Entities Deployed Across Multiple Nodes .....	51
Messaging Bus Not Required - Single Application Deployed to Single Node .....	51
Messaging Bus Not Required - Single Application Deployed Across All Nodes And Each Node is Distributed with All Entities of the Application .....	52
Service Probe Architecture .....	181
Current release of ActiveMatrix .....	277

# 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 ActiveMatrix® Service Grid is available on the <https://docs.tibco.com/products/tibco-activematrix-service-grid> page.

Use of the following features, installation profiles and development tools requires a TIBCO ActiveMatrix Service Grid license:



- TIBCO ActiveMatrix Policy Director Governance, TIBCO ActiveMatrix SPM Dashboard, and TIBCO ActiveMatrix SPM Runtime Server profiles; and
- TIBCO ActiveMatrix Service Grid development tools for Java, Webapp and Spring components.

Customers with only a TIBCO ActiveMatrix Service Bus license are not licensed to use these features, tools or profiles.

The following documents form the documentation set:

- *TIBCO ActiveMatrix Service Grid Concepts*: Read this manual before reading any other manual in the documentation set. This manual describes terminology and concepts of the platform. The other manuals in the documentation set assume you are familiar with the information in this manual.
- *TIBCO ActiveMatrix Service Grid Development Tutorials*: Read this manual for a step-by-step introduction to the process of creating, packaging, and running composites in TIBCO Business Studio.
- *TIBCO ActiveMatrix Service Grid Composite Development*: Read this manual to learn how to develop and package composites.
- *TIBCO ActiveMatrix Service Grid Java Component Development*: Read this manual to learn how to configure and implement Java components.
- *TIBCO ActiveMatrix Service Grid Mediation Component Development*: Read this manual to learn how to configure and implement Mediation components.
- *TIBCO ActiveMatrix Service Grid Mediation API Reference*: Read this manual to learn how to develop custom Mediation tasks.
- *TIBCO ActiveMatrix Service Grid Spring Component Development*: Read this manual to learn how to configure and implement Spring components.
- *TIBCO ActiveMatrix Service Grid WebApp Component Development*: Read this manual to learn how to configure and implement Web Application components.
- *TIBCO ActiveMatrix Service Grid REST Binding Development*: Read this manual to learn how to configure and implement REST components.
- *TIBCO ActiveMatrix Service Grid Administration Tutorials*: Read this manual for a step-by-step introduction to the process of creating and starting the runtime version of the product, starting TIBCO ActiveMatrix servers, and deploying applications to the runtime.
- *TIBCO ActiveMatrix Service Grid Administration*: Read this manual to learn how to manage the runtime and deploy and manage applications.

- *TIBCO ActiveMatrix Service Grid Hawk ActiveMatrix Plug-in*: Read this manual to learn about the Hawk plug-in and its optional configurations.
- *TIBCO ActiveMatrix Service Grid Policy Director Governance Custom Actions*: Read this manual to learn how you can configure and enforce policies for ActiveMatrix and external services hosted in third party containers, using TIBCO ActiveMatrix Policy Director Governance.
- *TIBCO ActiveMatrix Service Grid Service Performance Manager API Reference*: Read this manual to learn how to use the SPM APIs.
- *TIBCO ActiveMatrix Service Grid Error Codes*: Read this manual to know more about the error messages and how you could use them to troubleshoot a problem.
- *TIBCO ActiveMatrix Service Grid Installation and Configuration*: Read this manual to learn how to install and configure the software.
- *TIBCO ActiveMatrix Service Grid Security Guidelines*: Read this manual to learn more about security guidelines and recommendations for TIBCO ActiveMatrix Service Grid.
- *TIBCO ActiveMatrix Service Grid 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](https://community.tibco.com). For a free registration, go to <https://community.tibco.com>.

# Setting Up an Enterprise

---

A TIBCO ActiveMatrix® enterprise consists of a TIBCO ActiveMatrix® Administrator Server, one or more TIBCO Hosts, and one or more ActiveMatrix nodes either on a single machine or spread across multiple machines. This section explains what you need to set up an enterprise on a single machine or on multiple machines.

Depending on the type of installation required, you need to meet the installation requirements and pre-requisites summarized below:

## A Trial, Demonstration, or Educational Installation

This is the simplest configuration with minimal dependencies, a single user and on a single machine. You need:

- An EMS server instance dedicated to the ActiveMatrix installation.
- To meet installation requirements given in the [Installation Requirements](#) section.
- Install the product software on disk.
- Run TIBCO Configuration Tool, choosing an **Express Configuration** to create ActiveMatrix Administrator using the built-in HSQLDB database.
- Start TIBCO Business Studio to develop ActiveMatrix composite applications.
- Use `http://localhost:port/amxadministrator` to connect to ActiveMatrix Administrator.

## A Development, or Integration Test installation

This is a robust set up with multiple users, multiple developers on one or more machines. Typically you will have multiple ActiveMatrix developers using the TIBCO Business Studio developing applications locally, but deploying their applications for testing to a central ActiveMatrix Administrator Server accessible to all the developers.

On the developer machines, you will need:

- To meet installation requirements given in the [Installation Requirements](#) section.
- Install the product software on disk, choosing **TIBCO Business Studio** component.
- Start TIBCO Business Studio and develop ActiveMatrix composite applications.

On the ActiveMatrix Administrator machine, you need:

- An EMS server instance dedicated to the ActiveMatrix installation.
- A database server such as Oracle, Microsoft SQL Server, and so on with some pre-requisites met.
- To meet installation requirements given in the [Installation Requirements](#) section.
- Install the product software on disk.
- Run TIBCO Configuration Tool, choosing the following sequence of workflows:
  - Configure Third-party Driver
  - Create ActiveMatrix Administrator Server
  - (optional) Create TIBCO Host instance
  - Connect to `http://<admin-machine>:port/amxadministrator`, creating new user accounts as needed for each developer.

Then on TIBCO Business Studio, developers can register `http://<admin-machine>:port/amxadministrator` as the deployment server and directly deploy applications developed in TIBCO Business Studio.

**A Staging, Pre-Production, or Production Installation**

This is a robust set up with multiple users, fault-tolerant ActiveMatrix Administrator, multiple TIBCO Hosts on one or more machines.



# Installation Overview

---

Before proceeding with the actual installation, you must get familiar with installation modes, installation types, prerequisites, and profiles.

## Installation Modes

Three installation modes are available: GUI, console, and silent.

### GUI Mode

In the GUI mode, the installer presents panels using which you can select a product, its location, and so on. To invoke the installer in the GUI mode, double-click the executable.

### Console Mode

You can use the Console mode to run the installer from the command prompt or terminal window. This is useful if your machine does not have a GUI environment.

### Silent Mode

You can use the silent mode to install the product using either default or custom settings that are saved in a response file. The silent mode installs the product without prompting you for information.

## Installation Types

Two installation types are available: Profile or Custom.

- The Profile installation type installs all the software for a specific profile.
- The Custom installation type enables you to select components.

## Installer Log File

The installer log file, `tibco_universal_installer.username_install.log`, is written to the `.TIBCO/install_timestamp` folder of the user's home directory.

To change the location of the installer log file, specify the option `-V logFile="myLogFile"` when you run the installer.

The installer log file captures the following information:

- Installation environment details such as the user that invoked the installer, host name, Java home in the environment, operating system details, and so on
- List of assemblies installed

# Installation Requirements

Before running the installer on Windows or Linux systems, you must log in as a user with appropriate permissions, and ensure your system meets the hardware and software requirements as described in the following sections.

If you plan on installing in an existing installation environment, stop all processes that use Java from `TIBCO_HOME`.

Before you run the installer, see the `readme.txt` for information about the supported operating system platforms, versions, and the required patches if any.

## Installation Account Requirements

To install on Microsoft Windows or on UNIX, you must have the appropriate privileges.

The required privileges are different for different platforms.

- **Microsoft Windows** - Only users with administrator privileges can install the TIBCO ActiveMatrix products. If you do not have administrator privileges, the installer exits. To install the product on a network drive, ensure that the account used for installation has the permission to access the network drive.



On UAT-enabled Windows platforms, non-default administrators may encounter permission issues under certain circumstances. To avoid permission issues, start the TIBCO Universal Installer, TIBCO Configuration Tool, and Command Prompt with the **Run as Administrator** option.

- **UNIX** - Any type of user—regular (non-root) user and super-user (root)—can install the product. Use the same installer account to install all the TIBCO ActiveMatrix products. A graphic environment such as CDE or X Windows is required to run the installer in the GUI mode.



For configuration, the user who runs the TIBCO Configuration Tool must also have administrator privileges on the TIBCO Enterprise Message Service servers that you want to use in your TIBCO ActiveMatrix enterprise. If you do not have administrator privileges, you can configure using additional setup. See [Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users](#).

## Hardware Requirements

The installation requires a substantial amount of system memory and disk space.

Review the system memory and disk space requirements before you start installing.

### System Memory

A minimum of 4 GB (8 GB recommended) of physical memory is required.

### Disk Space

The installer requires some space in the temporary directory before installation, as well as additional space in the temporary directory for running the installer. You must also make sure that the directory you want to use for the installation environment (`TIBCO_HOME`) has sufficient space.



While installing, avoid running other processes that consume disk space in the installation environment directory. If another process consumes disk space while the installer is copying the files, the installer might fail with an error.

Directory	Disk Space Requirement
Temporary directory before installation For example, c:\temp	Before you start the installation, you need this space to download the installer archive file. The installer archive file can consume up to 990 MB of disk space.
Temporary directory during installation For example, c:\temp\amx340	<p>This is the directory where you must extract the installer archive file so that you can later execute the Universal Installer. The installer requires at least 275 MB of free space in the temporary directory.</p> <p>On Microsoft Windows, the default temporary directory location is %SystemDrive%\Documents and Settings\user_name\Local Settings\Temp.</p> <p>If your system does not have sufficient free disk space in the default temporary directory, you can use the <code>is:tempdir</code> option to run the installer with a different temporary directory. For example:</p> <pre><b>TIBCOUniversalInstallerPlatform</b> -is:tempdir \new_tmp</pre> <p>where \new_tmp is the directory that has sufficient free disk space.</p>
Installation environment directories	The installer calculates the disk space required in the installation environment directory for the selected components. The calculation is done before the actual installation (copying of files to system) begins. The installer proceeds only if sufficient free disk space is available in the installation environment directory. A TIBCO ActiveMatrix product might consume 1GB of free space under <i>TIBCO_HOME</i> .

## Software Requirements

Your system must meet the software requirements before you run the installer. Some software is required and others are optional. An external database is required for production systems but not during development.

Before you run the installer, you must make sure you are running on a supported platform. See the *Readme* file for information about the supported operating system platforms and versions and about required patches.

You must also have required software installed. See the *Readme* file for the supported products and versions.


[Required and Optional Software](#) lists the required and optional software. Several of the required software components are downloaded by the installer.


### Required and Optional Software




When you obtain third party software or services, it is your responsibility to ensure you understand the license terms associated with such third-party software or services and comply with such terms.

Software	Description
Hibernate	Required. If necessary, the TIBCO Universal Installer automatically downloads Hibernate during installation.

Software	Description
Eclipse components	Required. On some operating system platforms, TIBCO Universal Installer automatically downloads certain Eclipse LGPL components during installation if necessary.
JRE Components	<p>On some operating system platforms, you must download Oracle Java 8 Elliptic Curve Cryptography (ECC) LGPL separately. Oracle ships the SunEC (an ECC implementation) library as part of JRE 8. The SunEC library is covered by a different license (LGPL). Install this library to take advantage of ECC. The TIBCO Universal Installer automatically downloads the library for you from <code>download.tibco.com</code> during installation.</p> <p>If you do not want to install the Elliptic Curve Cryptography library, delete the library named <code>libsunec.so</code> (on Solaris and Linux systems) or <code>sunec.dll</code> (on Windows systems) or <code>libsunec.dylib</code> (on MacOS) from the <code>TIBCOJRE</code> bin directory, reserved for native libraries.</p> <div>  <div>IBM's implementation of Java 8 includes ECC, but ECC does not fall under a separate license as it does in Oracle's implementation.</div> </div>
TIBCO Software	<p>Several software components from TIBCO Software might be required. Some components are included in the installer package, others must be installed separately. See the <i>Readme</i> file for details about the required versions.</p> <ul style="list-style-type: none"> <li>• <b>Java Virtual Machine</b> - Required. JRE 8 is included in the installation. Alternatively, you can also use the JRE version already installed on your machine.</li> <li>• <b>TIBCO Enterprise Message Service</b> - Required. This software is not included in the installer package and must be installed separately. This software is used as: <ul style="list-style-type: none"> <li>– the notification and messaging backbone for the TIBCO ActiveMatrix products</li> <li>– the messaging transport by both the TIBCO Service Performance Manager (SPM) server and the TIBCO ActiveMatrix SPM dashboard server for communicating statistics. When and where the EMS server is installed affects the configuration of TIBCO ActiveMatrix SPM dashboard server.</li> </ul> <p>At least one EMS server must be installed on the network that can be used with TIBCO Service Performance Manager.</p> </li> <li>• <b>TIBCO Hawk</b>: Hawk allows you to monitor and manage distributed applications and systems throughout the enterprise.</li> </ul>

Software	Description
OpenJDK	<p>TIBCO ActiveMatrix Service Grid 3.4.0 supports OpenJDK (Amazon Corretto 8, update 212) on Windows (64-bit) and Linux (64-bit) operating systems for the following installation profiles:</p> <ul style="list-style-type: none"> <li>• Administrator</li> <li>• Runtime Host</li> <li>• SOA Development</li> </ul> <p>You can download and install Amazon Corretto 8 from <a href="#">Amazon Web Services Website</a>.</p> <p>To use OpenJDK, select the option <b>Specify Currently Installed Java</b> in the Java Home screen of the installer wizard. Click <b>Browse</b> to navigate to the directory where Amazon Corretto 8 is installed.</p> <p>Alternatively, you can use TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) to configure existing setup to use Amazon Corretto 8. For more information, see <a href="#">Updating JRE Version</a>.</p>
Tomcat Web Server	<p>Tomcat is not a prerequisite during the installation process; it will be installed on your machine when TIBCO ActiveMatrix is installed. The Tomcat web server is necessary to host the SPM dashboard.</p>
Database Software	<p>Required to store administration information. For a list of supported databases, see the <i>Readme</i> file.</p> <p>An embedded version of HSQLDB is included for demonstration and trial setups.</p> <div>  <p>HSQLDB must not be used for production or any setup where data loss is unacceptable. This version of HSQLDB does not guard against database corruption.</p> </div>
JDBC Drivers	<p>Required by TIBCO ActiveMatrix Administrator and by associated services to access the database resources. For the supported drivers, see the <a href="#">Third-Party Driver Details</a> section.</p> <p>If you use the embedded version of HSQLDB during development, you do not have to install a third-party driver.</p>
LDAP Servers	<p>Optional. Supports the LDAP authentication realm that the Administrator server can use for authenticating users. As an alternative, you can configure a database authentication realm.</p>
JMS Servers	<p>Optional. Supports SOAP/JMS and JMS binding types.</p>
Web Browser	<p>Required to run the ActiveMatrix Administrator GUI. See the <i>Readme</i> for a list of supported browsers.</p>
Apache Ant	<p>Required to run TIBCO Configuration Tool, runtime object upgrade, and ActiveMatrix Administrator CLI scripts.</p> <p>Apache Ant 1.9.9 is bundled as a part of ActiveMatrix under TIBCO_HOME\amx\&lt;version&gt;\bin\ant. This Ant can be used by adding TIBCO_HOME\amx\&lt;version&gt;\bin to the environment variable PATH.</p>

Software	Description
GTK2	<p>On some UNIX and Linux platforms, you must install the GTK2 libraries and their dependencies and make them available in the library path (LD_LIBRARY_PATH). To determine the full set of libraries required for installation, download and install the gtk2 rpm. All missing dependencies are listed. These dependencies are available for download from the GTK2 download site.</p> <p> You must use GTK 2.24.0 or a later version with Eclipse 4.7 (Oxygen).</p>

## Database Requirements for SPM

There are some limitations observed while working with DB2 and MS SQL Server.

### DB2 Requirements

If you are using DB2 for data persistence, use the following configuration:

- Set the table space size to 32k. For example,  

```
CREATE DATABASE <spm db> AUTOMATIC STORAGE YES ON 'C:/' USING CODESET IBM-1252
TERRITORY US COLLATE USING SYSTEM PAGESIZE 32768;
```
- Set the Bufferpool to 32k.

### MS SQL Server Requirements

- Enable SNAPSHOT transaction isolation for MS SQL Server database.  

To enable READ\_COMMITTED\_SNAPSHOT for the Service Performance Manager database, run the following commands as Database System Administrator (sa):

```
ALTER DATABASE <spmDB name> SET READ_COMMITTED_SNAPSHOT ON;
ALTER DATABASE <spmDB name> SET ALLOW_SNAPSHOT_ISOLATION ON;
```
- When using SQL Server, ensure that you use case sensitive collation. You may enable case sensitive collation using a command similar to the following:  

```
CREATE DATABASE spm COLLATE SQL_Latin1_General_CP1_CS_AS;
```

Refer to the SQL Server documentation for more information regarding collation.

## Installation Environment

Before installation, make sure the system meets all the prerequisites. First, decide on the installation environment and folder and then download and extract the installation package.

- TIBCO\_HOME* is the top-level installation directory for TIBCO products.
- TIBCO\_HOME* is referred to as the installation environment.

Installation environments isolate product installations; a product installed into an installation environment does not automatically access components in other environments.

An installation environment consists of a name and a folder.

- The name identifies the environment and it is appended to the name of the Windows services created by the installer. It is a component of the path to the product in the Windows **Start > All Programs** menu.
- The folder contains the installed software. When you install, you can choose a new installation environment or an existing installation environment.


Set up the installation environment as follows:

Option	Description
If a previous installation of the TIBCO product did not use the TIBCO Universal Installer	The TIBCO Universal Installer does not detect the folder it uses as an installation environment folder. If you wish to use the existing location as the installation folder, create a new installation environment and choose the folder where the other products exist.
If you plan on installing in an existing installation environment	Stop all processes that are using Java from <code>TIBCO_HOME</code>
If you plan on installing on a machine on which runtime objects (Administrator server, TIBCO Host instances, and nodes) are running	Stop all the processes corresponding to the objects.
If you plan on installing the SOA Development profile or a custom profile containing TIBCO Business Studio	Create a new installation environment

## Installation Profiles

During custom installation, you can choose from the following installation profiles. Depending on the profile you choose, select components are installed.

### *Installation Profiles of ActiveMatrix Service Grid*

Component	Description
Administration	Includes TIBCO ActiveMatrix Administrator and Mediation Runtime. Install this profile to create TIBCO ActiveMatrix Administrator servers on the machine.
Runtime Host	Includes TIBCO Host software. Install this profile to create TIBCO Host instances on the machine.
SOA Development	Includes TIBCO Business Studio, Composite Editor, Mediation Flow Editor, binding and implementation type editors. Install this profile to develop TIBCO ActiveMatrix applications on the machine.  <div>  <div>Do not install a new TIBCO Business Studio on an existing <code>TIBCO_HOME</code> (with an older version of TIBCO Business Studio). Install TIBCO Business Studio in a separate <code>TIBCO_HOME</code>.</div> </div>
TIBCO ActiveMatrix PD Governance	Includes TIBCO ActiveMatrix Policy Director Governance Services and proxy hosts.
TIBCO ActiveMatrix SPM Dashboard Server	Includes the TIBCO ActiveMatrix Dashboard application to display aggregated and computed key performance indicators (KPI) in easy-to-understand dashboard layouts for TIBCO ActiveMatrix.

Component	Description
TIBCO ActiveMatrix SPM Runtime Server	<p data-bbox="555 226 1203 254">Includes the TIBCO ActiveMatrix SPM runtime server.</p> <div data-bbox="555 281 596 323"></div> <p data-bbox="671 281 1426 338">Managing and monitoring performance of TIBCO ActiveMatrix BPM services is not supported using SPM.</p>



## Pre-installation

Pre-installation tasks include customizing your environment for certain platforms. In a production environment, you must set up an external database before installation because the database included in the installation is supported only for development.

### Configuring External Databases

The in-process HSQLDB database must only be used in trial setups where data loss is acceptable. If not, you must use an external database with your ActiveMatrix enterprise.

**Prerequisite:** If you are using an external database, you have to perform database-specific configuration before you can create runtime objects such as the Administrator server.

Set up your database, depending on the database vendor. The database schema can either be created automatically or manually. The DDL Script Generator utility generates the database scripts that can be executed manually. The database permissions needed will vary accordingly.

To create an ActiveMatrix Administrator server, you must provide database information including a database username. This database user account needs the right privileges for proper operation.

#### *Permissions Needed to Create the Database Schema*

Creation of The Database Schema	Database Privileges Needed
Automatically	<ol style="list-style-type: none"> <li>1. Grant DDL privileges, such as permissions to access create tables, indexes, constraints, and so on to the database user account.</li> <li>2. Grant DML privileges, such as permissions to select, insert, update, delete records in the tables, or query for table meta-data.</li> </ol> <p>The permissions are specific to the database type and are listed under <a href="#">Database Permissions Needed for Automatic Schema Creation</a>.</p>
Manually	<p>Grant DML privileges, such as permissions to select, insert, update, delete records in the tables, or query for table meta-data. The permissions are specific to the database type and are listed under <a href="#">Database Privileges Needed for Manual Schema Creation</a>.</p>

### Database Privileges Needed for Automatic Schema Creation

Lists the privileges needed specific to database type for automatic schema creation.

#### *Privileges Granted Based on the Database Type*

Database Type	Privileges
Oracle	<p><b>Required :</b> You must not have the DBA privilege, and you must be assigned to the database schema.</p> <p><b>Permissions:</b> grant connect, resource to &lt;amx-user&gt;.</p>

Database Type	Privileges
Microsoft SQL Server	<p><b>Required:</b> Set 'read_committed_snapshot' to ON by executing:</p> <ol style="list-style-type: none"> <li>1. alter database &lt;amx-database&gt; set read_committed_snapshot on</li> <li>2. Use the case insensitive collation setting for &lt;amx-database&gt;</li> <li>3. Assign &lt;amx-user&gt; the default database &lt;amx-database&gt;</li> </ol> <p><b>Permissions:</b> grant db_owner role to &lt;amx-user&gt; for the &lt;amx-database&gt;.</p>
IBM DB2	<p><b>Required:</b> Configure the database with a 32KB page size (instead of the default 4KB page size).</p>
PostgreSQL (Starting with TIBCO ActiveMatrix Hotfix 002)	<ol style="list-style-type: none"> <li>1. Create the database user using pgAdmin or SQL Shell and grant the required privilege.</li> <li>2. Create the database. The user created in the step 1 must be the owner of the database.</li> <li>3. In pgAdmin or SQL shell, run the following queries for the database created in the step 2 : <pre>CREATE FUNCTION pg_catalog.text(bigint) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int8out(\$1));'; CREATE CAST (bigint AS text) WITH FUNCTION pg_catalog.text(bigint) AS IMPLICIT;  CREATE FUNCTION pg_catalog.text(integer) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int4out(\$1));'; CREATE CAST (integer AS text) WITH FUNCTION pg_catalog.text(integer) AS IMPLICIT;  CREATE FUNCTION pg_catalog.text(smallint) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int2out(\$1));'; CREATE CAST (smallint AS text) WITH FUNCTION pg_catalog.text(smallint) AS IMPLICIT;</pre> </li> </ol>

**Postrequisite:** After installation, you have to use TIBCO Configuration Tool to configure the third-party JDBC driver for your database.

## Database Privileges Needed for Manual Schema Creation

Lists the privileges needed specific to database type for manual schema creation.

### *Privileges Granted Based on the Database Type*

Database Type	Privileges
Oracle	<p><b>Required :</b> You must not have the DBA privilege, and you must be assigned to the database schema.</p> <p><b>Permissions:</b> Grant the following permissions:</p> <pre>grant create session</pre>

Database Type	Privileges
Microsoft SQL Server	<p><b>Required:</b> Set 'read_committed_snapshot' to ON by executing:</p> <ol style="list-style-type: none"> <li>1. alter database &lt;amx-database&gt; set read_committed_snapshot on</li> <li>2. Use the case insensitive collation setting for &lt;amx-database&gt;</li> <li>3. Assign &lt;amx-user&gt; the default database &lt;amx-database&gt;</li> </ol> <p><b>Permissions:</b> grant db_datareader, db_datawriter to &lt;amx-user&gt; for the &lt;amx-database&gt;.</p>
IBM DB2	<p><b>Required:</b> Configure the database with a 32KB page size (instead of the default 4KB page size).</p> <p><b>Permissions:</b> Create dmluser with connect database permission.</p>
PostgreSQL (Starting with TIBCO ActiveMatrix Hotfix 002)	<ol style="list-style-type: none"> <li>1. Create the database user using pgAdmin or SQL Shell and grant required privilege.</li> <li>2. Create the database. The user created in the step 1 must be the owner of the database.</li> <li>3. In pgAdmin or SQL shell, run the following queries for the database created in the step 2 : <pre>CREATE FUNCTION pg_catalog.text(bigint) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int8out(\$1));'; CREATE CAST (bigint AS text) WITH FUNCTION pg_catalog.text(bigint) AS IMPLICIT;  CREATE FUNCTION pg_catalog.text(integer) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int4out(\$1));'; CREATE CAST (integer AS text) WITH FUNCTION pg_catalog.text(integer) AS IMPLICIT;  CREATE FUNCTION pg_catalog.text(smallint) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int2out(\$1));'; CREATE CAST (smallint AS text) WITH FUNCTION pg_catalog.text(smallint) AS IMPLICIT;</pre> </li> </ol>

To run the DDL Script Generator utility, see [DDLGeneratorTask](#).

### What to do next

After installation, use TIBCO Configuration Tool to configure the third-party JDBC driver for your database.

## Configuring Ant

The default setup of Ant might have an insufficient amount of memory available for running CLI scripts or configurations scripts from the TIBCO Configuration Tool. You can increase the value for your Windows or Linux system.

Confirm the value of `ANT_OPTS` before you execute scripts from the command prompt.

- **Windows** Edit %USERPROFILE%\antrc\_pre.bat and add following line:

```
set ANT_OPTS=-Xmx1024m
```

- **UNIX** Edit ~/.antrc and add the following line:

```
export ANT_OPTS="-Xmx1024m"
```

## Configuring AIX Platforms

On AIX, change the maximum allowable size of the ARG/ENV list. If you do not change, TIBCO Host instances cannot start.

### Prerequisites

If you installed a product that supports AIX 6.1 and you want to use that platform, you must install several prerequisite packages.

See the Readme file for your product for a list of supported platforms. This document may describe platforms that are not supported for your product.

### Procedure

1. Log in as root.
2. Open a terminal window, and run the following command.

```
chdev -l sys0 -a ncargs=16
```

## Configuring the Environment Settings for AIX Platforms Versions

To run native executables such as, a wrapper that launches Java, requires special configuration on AIX. This section lists the environment variables that should be set to improve the performance on AIX.

Following are some configuration parameters that may affect the performance and memory profile of ActiveMatrix and Business Process Management nodes. For details, refer to [https://www.ibm.com/support/knowledgecenter/SSYKE2\\_8.0.0/welcome/welcome\\_javasdk\\_version.html](https://www.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/welcome/welcome_javasdk_version.html) for details on *Running Java Applications* for Java Version 8 on the AIX platform.

### Setting the Java Heap Size

The `maxdata` setting controls the size of the Java heap used by the executable launching the JVM (AMX or BPM Node). The ActiveMatrix and Business Process Management node executables are compiled with `maxdata` value of `0x80000000`. This value can be changed by running the following command:

```
ldedit -bmaxdata:<value> tibamx_BPMNode
```

where `<value>` is the value of the `maxdata`; this value can be changed to be unlimited.

### Setting the Environment Variables That Have an Impact on JVM Runtime

On AIX, here are some environment variables that have an impact on the JVM runtime:

`LDR_CNTRL=USERREGS`: Used to set the `modType` flag to `1L`. This improves the performances of the garbage collector.

The following environment variables are suggested by IBM to improve the performance of JVM.

- `AIXTHREAD_SCOPE=S`
- `AIXTHREAD_MUTEX_DEBUG=OFF`
- `AIXTHREAD_RWLOCK_DEBUG=OFF`
- `AIXTHREAD_COND_DEBUG=OFF`

The `AIXTHREAD_SCOPE=S` environment variable is used to bind a user thread to a dedicated kernel thread. If omitted the default behavior is to bind multiple user threads with a single kernel thread. This can cause both concurrency and performance issues. Refer to the IBM documentation for details on the usage of each of these environment variables.

## Configuring the Maximum Number of Open Files on Linux Platforms

Your Linux platform default settings might have a limit on the maximum number of open files and file descriptors that is too low for the product you want to install. You can change this number by editing the `limits.conf` configuration file.

On all Linux systems, the operating system controls the maximum number of open files and file descriptors. The threshold is typically too low and must be increased. The exact number depends on the features you select during installation and configuration and on the size of the workspace. In most cases, 10000 files is sufficient.

### Procedure

1. Edit `/etc/security/limits.conf` and add the following line:  
     \* **hard nofile 10000**
2. Log out of the system and log back in.

## Downloading Software Assemblies if No Internet Access is Available

If your machine will not be connected to the Internet during installation, you must download several software assemblies from the TIBCO download site before you start the installation process. Download the assemblies after you download and extract the installer, but before you run the installer.

### Procedure

1. Decide on the download location for the assemblies.
  - To streamline the process, save the software assemblies to the `assemblies` subdirectory of the temporary directory that you extracted the installer package in.
  - You can also download the assemblies to a different temporary directory.
2. To download the Hibernate software assembly, click **TIB\_assembly\_tibco\_com\_tibco\_tpcl\_org\_hibernate\_feature\_3.2.500.002\_all.html** on the TIBCO download site.  
`assembly_tibco_com_tibco_tpcl_org_hibernate_feature_3.2.500.002.zip` is downloaded to the location you select.
3. On Linux, HP, AIX, and Solaris, download the following Eclipse LGPL software assemblies from the TIBCO download site.  
 In the following steps, *OSplatform* is one of `linux_x86_64`, `sol_sparc_64`, `sol_x86_64`, `aix_power_64`, or `hpux_ia64`.
  - a) Click **TIB\_product\_tibco\_eclipse\_lgpl\_4.7.1.001\_OSplatform.html**.  
`product_tibco_eclipse_lgpl_4.7.1.001_OSplatform.zip` is downloaded to the location you select.
  - b) Click **TIB\_product\_tibco\_eclipse\_lgpl\_rcp\_4.4.2.001\_OSplatform.html**.  
`product_tibco_eclipse_lgpl_rcp_4.4.2.001_OSplatform.zip` is downloaded to the location you select.
  - c) Click **TIB\_product\_tibco\_sunec\_1.8.0.192\_OSplatform.html**.  
`product_tibco_sunec_1.8.0.192_OSplatform.zip` is downloaded to the location you select.

## Installation and Configuration Checklist

Lists a set of tasks needed to install and configure the product.

### Checklist

Stages	Steps
Preinstallation	<ol style="list-style-type: none"> <li>1. <a href="#">Installation Requirements</a></li> <li>2. <a href="#">Hardware Requirements</a></li> <li>3. <a href="#">Software Requirements</a></li> <li>4. <a href="#">Configuring External Databases</a></li> <li>5. <a href="#">Configuring ANT</a></li> <li>6. <a href="#">Configuring AIX Platforms</a></li> <li>7. <a href="#">Configuring the Maximum Number of Open Files on Linux Platforms</a></li> <li>8. <a href="#">Downloading Software Assemblies if No Internet Access is Available</a></li> </ol>
Installation	<p>Choose one of the following ways of installing the product:</p> <ol style="list-style-type: none"> <li>1. <a href="#">Installing in GUI Mode</a></li> <li>2. <a href="#">Installing in Console Mode</a></li> <li>3. <a href="#">Installing in Silent Mode</a></li> </ol>
Post-installation	<p>After installation, ensure that Enterprise Messaging Service is up and running before starting TIBCO Configuration Tool. For details, see:</p> <ol style="list-style-type: none"> <li>1. <a href="#">TIBCO Configuration Tool Requirements</a></li> <li>2. <a href="#">Enterprise Messaging Server Requirements</a></li> <li>3. <a href="#">SSL Requirements</a></li> </ol>

Stages	Steps
Configuration	<p>The configuration steps vary based on your needs.</p> <ol style="list-style-type: none"> <li>1. If you are using external databases, configure the third party driver by following the steps in <a href="#">Configure Third-Party Driver</a>.</li> <li>2. Before this step, make sure that the EMS server is up and running. There are two ways of creating the TIBCO ActiveMatrix Administrator Server:             <ol style="list-style-type: none"> <li>a. If you want to select the default settings, follow the steps in <a href="#">Create Express Developer Environment</a>.</li> <li>b. Before this step, ensure that you have configured the external database and configured the third-party driver. To customize the port, environment, and database settings, follow the steps in <a href="#">Create TIBCO ActiveMatrix Administrator Server</a>.</li> </ol> </li> <li>3. If you have ActiveMatrix Administrator on one machine and the TIBCO Host on another machine, and they share the same EMS server, follow the steps in <a href="#">Create TIBCO Host Instance</a>.</li> <li>4. For high availability, it is a best practice to replicate ActiveMatrix Administrator. See <a href="#">Replicate TIBCO ActiveMatrix Administrator Server</a>.</li> </ol>

# Installing TIBCO ActiveMatrix Service Grid

---

Install TIBCO ActiveMatrix Service Grid using the TIBCO Universal Installer. The installer runs on multiple platforms. You can run the installer in the GUI mode, console mode, and silent mode.

## Installing in GUI Mode

When you run the installer in the GUI mode, the installer prompts you for information about the installation environment, and allows other customizations.

### Prerequisites

Prepare your system for the installation. See [Installation Requirements](#) and [Pre-installation Tasks](#).

### Procedure

1. Download the installer package.
2. Extract the contents of the installer package to a temporary directory.
3. Navigate to the temporary directory.
4. Run **TIBCOUniversalInstaller**.
5. Click **Next** on the Welcome screen.
6. Read through the license agreement, select **I accept the terms of the license agreement**, and click **Next**.
7. Follow these steps to accept license agreements for third-party software and to optionally install that software.
  - a) When the Hibernate license agreement appears, read the text and click **I accept the terms of the license agreement**.
  - b) On Linux and Solaris, the LGPL License Agreement appears. Read the text and click **I accept the terms of the license agreement**.
  - c) If the Hibernate software is not in the `assemblies` subdirectory of your temporary directory, you are prompted for a Download Hibernate option.



- **Download Hibernate assembly from TIBCO.** Select this option if you are connected to the Internet or you do not want to use a previously downloaded assembly. The assembly is automatically downloaded and stored in the `assemblies` subdirectory of the directory where you extracted the installer.
- **Select the Hibernate assembly previously downloaded from TIBCO.** Choose this option if you are not connected to the Internet. Click **Browse** to navigate to the directory where a Hibernate assembly that was previously downloaded is stored and click **Open**. See [Downloading Software Assemblies if No Internet Access is Available](#).

To download Hibernate, the wizard displays the Hibernate download process.

- d) On Linux and Solaris, if you install Development Tool, and if the `product_tibco_eclipse_lgpl_4.7.1.001` (Linux) and `product_tibco_eclipse_lgpl_4.4.1.001` (Solaris) assemblies are not in the `assemblies` subdirectory of your temporary directory, the LGPL Assembly Download screen displays. Select a download option:
  - **Download Gnome Binding assembly from TIBCO.** Select this option if you are connected to the Internet or do not want to use a previously downloaded assembly. The assembly is automatically downloaded and stored into the `assemblies` subdirectory of the directory where you extracted the installer.



- **Provide the location for the assembly previously downloaded from TIBCO.** Select this option if you are not connected to the Internet. Click **Browse** to navigate to the directory where the `product_tibco_eclipse_lgpl_4.7.1.001` assembly that was previously downloaded is stored. Select the assembly and click **Open**. See [Downloading Software Assemblies if No Internet Access is Available](#).
- e) On Linux and Solaris, if you install TIBCO Host software and the `product_tibco_eclipse_lgpl_rcp_4.4.2.001` assembly is not in the `assemblies` subdirectory of your temporary directory, the LGPL Assembly Download screen displays. Select a download option:
- **Download GNOME Binding assembly from TIBCO.** Select this option if you are connected to the Internet or do not want to use a previously downloaded assembly. The assembly is automatically downloaded and stored into the `assemblies` subdirectory of the directory where you extracted the installer.
  - **Provide the location for the assembly previously downloaded from TIBCO.** Select this option if you are not connected to the Internet. Click **Browse** to navigate to the directory where the `product_tibco_eclipse_lgpl_rcp_4.4.2.001` assembly that was previously downloaded is stored. Select the assembly and click **Open**. See [Downloading Software Assemblies if No Internet Access is Available](#).
8. On the Installation Profile Selection screen, select one or more of the previously configured profiles, or click **Customize Installation** and explicitly select the components you want to install. Click **Next**.

Option	Description
<b>Administration</b>	Includes TIBCO ActiveMatrix Administrator, Mediation Runtime, and supporting documentation for each product. Install this profile to create TIBCO ActiveMatrix Administrator servers on the machine.
<b>Runtime Host</b>	Includes TIBCO Host software and supporting documentation. Install this profile to create TIBCO Host instances on the machine.
<b>SOA Development</b>	Includes TIBCO Business Studio, Composite Editor, Mediation Flow Editor, binding and implementation type editors, and supporting documentation. Install this profile to develop TIBCO ActiveMatrix applications on the machine.
<b>TIBCO ActiveMatrix PD Governance</b>	This profile installs the following: <ol style="list-style-type: none"> <li>1. TIBCO ActiveMatrix Policy Director Governance Services</li> <li>2. TIBCO ActiveMatrix Policy Director Governance proxy host</li> </ol>
<b>TIBCO ActiveMatrix SPM Dashboard Server</b>	Select to install TIBCO ActiveMatrix SPM Dashboard Server  You must select at least one of the Administration or Runtime Host installation profiles with TIBCO ActiveMatrix SPM Dashboard Server.
<b>TIBCO ActiveMatrix SPM Runtime Server</b>	Select to install TIBCO ActiveMatrix SPM Runtime Server  Managing and monitoring performance of TIBCO ActiveMatrix BPM services is not supported using SPM.

9. From the Java Home screen, select a JVM provided by TIBCO or specify an existing installation of Java. Click **Next**.
10. Shut down all TIBCO processes if the installer prompts you to do so.  
 The installer prompts if the features are already installed on the target system. Reinstalling features is not usually recommended.

11. On the Pre-Install summary screen, verify the list of products selected for installation, and click **Install**.
12. (Optional) Select **Launch Configuration Tool** to start the configuration process after installation (for example: create TIBCO Host or Administrator server instances). If you want to configure the product later, you can skip this step for now.



To launch TIBCO Configuration Tool later, execute `TIBCO_HOME/amx/<version>/bin/TIBCOConfigurationTool`. Alternatively, you can also execute `TIBCO_HOME/tct/<version>/bin/TIBCOConfigurationTool`.

13. Click **Finish** to complete the installation process and exit the universal installer.

## Installing in Console Mode

After you prepare your system and the installation media, you can run the installer in the console mode.

### Prerequisites

Prepare your system for the installation. See [Installation Requirements](#) and [Pre-installation Tasks](#).

### Procedure

1. In a console window, navigate to the temporary directory to which you extracted the files.
2. Run **TIBCOUniversalInstaller -console**.  
The installer launches a second console window.
3. Respond to the prompts in the second console window.  
The installer prompts for installation information and you can return to a previous selection periodically. The process is similar to [Installing in GUI Mode](#).
4. When installation completes, press **Enter** to exit the installer.  
The console installer does not prompt you to run TIBCO Configuration Tool. To create servers and other runtime objects, you can run TIBCO Configuration Tool explicitly.

### What to do next

After you exit the installer, you perform post-installation tasks and configuration. To configure your environment, you can run TIBCO Configuration Tool in the GUI mode, console mode, or silent mode.

1. Continue with [Uninstallation](#).
2. Run TIBCO Configuration Tool. See [Configuration Tool Wizards and Screens](#).

## Installing in Silent Mode

In the silent mode, the installer does not prompt for inputs during installation but reads the inputs from a response file. By default, the installer uses the `TIBCOUniversalInstaller-product_version.silent` file, which is included in the directory that contains the universal installer.

### Prerequisites

Prepare your system for the installation. See [Installation Requirements](#) and [Pre-installation Tasks](#).

You can customize the silent installer as follows:

- Make a backup copy of the `TIBCOUniversalInstaller-product_version.silent` file and edit the file itself. You can then run the silent installer with or without the response file argument.

- Make a copy of the `TIBCOUniversalInstaller-product_version.silent` file and name the copy. You can then run the silent installer, passing in your custom response file.

### Procedure

1. Make a copy of the `TIBCOUniversalInstaller.silent` file and name the file, for example, *myfilename.silent*.
2. Using a text editor, open the copied file and update the installation location and features to install.
3. Run the silent installer with or without the optional response file.
  - **Windows:** `TIBCOUniversalInstaller.cmd -silent [-V responseFile="myfile.silent" ]`
  - **UNIX:** `TIBCOUniversalInstaller.bin -silent [-V responseFile='myfile.silent']`

### What to do next

After exiting the installer, perform the post-installation tasks and configuration. You can run TIBCO Configuration Tool in the GUI mode, console mode, or silent mode.

1. Continue with [Uninstallation](#).
2. Run TIBCO Configuration Tool.  
See [Configuration Tool Wizards and Screens](#).

## Moving an Installation to a Destination Machine

You can install the TIBCO ActiveMatrix products on a source machine and move the installed software and scripts to a destination machine. With this procedure, you can create TIBCO Host instances and Administrator server on destination machines without running the installer on each destination machine.

### Procedure

1. Install the product on the source machine.
2. If you are using the GUI installer, clear the **Launch TIBCO Configuration Tool** checkbox on the final installer panel.
3. Package the contents of `TIBCO_HOME` using an archive utility.
4. Unpack the archive on the target machine. Use the same location on the destination machine as you did on the source machine. For example: `C:\Program Files\tibco\amx-3`.
5. On the destination machine, run TIBCO Configuration Tool to create TIBCO Host instances and an ActiveMatrix Administrator server.

### What to do next

After you have moved the installation, you can run TIBCO Configuration Tool on each target machine to configure your setup.

## Verifying Installation

Ensure that the installation was successful by verifying that all the folders were successfully created by the installer in `TIBCO_HOME`.

For Service Performance Manager, the files are placed in `TIBCO_HOME/spm/2.3`.

## TIBCO\_HOME Files and Directories

After the product is installed, you can see the directory structure as shown in the following table.

### *TIBCO\_HOME Files and Directories*

Directory	Description	Contents
TIBCO_HOME/_installInfo	Contains information about all installed products	/assembly_registry
TIBCO_HOME/administrator	Contains information related to TIBCO ActiveMatrix Administrator. For example, scripts, schemas, samples, templates, and so on.	
TIBCO_HOME/amx	Contains information related to TIBCO ActiveMatrix Service Grid.	
TIBCO_HOME/amx_it_mediation	Contains information related to the Mediation Implementation Type. For example, scripts and samples.	
TIBCO_HOME/amxspmdashboard/<version>	Contains information related to the ActiveMatrix SPM Dashboard.	
TIBCO_HOME/amxspmdashboard/<version>/amxdashboard/	Contains the sh or bat files to start and stop the dashboard. It also includes the Tomcat server.	
TIBCO_HOME/amxspmdashboard/<version>/config	Contains the configuration files required by the Dashboard Server and Logger.	
TIBCO_HOME/amxspmdashboard/<version>/logs	Default folder for TIBCO ActiveMatrix SPM Dashboard server logs such as amxdashboard.log.	
TIBCO_HOME/amxspmdashboard/<version>/setup	Contains TIBCO ActiveMatrix SPM Dashboard server Post Install - automated setup script.	
TIBCO_HOME/amxspmdashboard/<version>/webconsole	Contains TIBCO ActiveMatrix SPM Dashboard Web Application archive (amxdashboard.war).	

Directory	Description	Contents
TIBCO_HOME/ amxspmdashboard/ <version>/lib	Contains TIBCO ActiveMatrix runtime library required for SPM server (amx-rtruntime.jar).	
TIBCO_HOME/components		
TIBCO_HOME/eclipse-platform		
TIBCO_HOME/ems	Contains information to TIBCO Enterprise Message Service.	
TIBCO_HOME/ogp		
TIBCO_HOME/p2repos		
TIBCO_HOME/pd	Contains information related to TIBCO ActiveMatrix Policy Director Governance.	
TIBCO_HOME/release_notes	Contains the readme and release notes of all the installed products	
TIBCO_HOME/spm/<version>	Contains all the TIBCO Service Performance Manager components	

Directory	Description	Contents
TIBCO_HOME/spm/ <version>/bin	Contains various executables for running the Server and example.	<p>tibspmexamples is a self-running example to demonstrate the various client APIs, and features.</p> <p>tibspmdllgenerator is a tool provided to generate various DDL and DML scripts for the chosen type of database.</p> <p>tibspm is the Service Performance Manager server.</p> <p>tibspmpassword is a password obfuscator that can be used to encrypt password credentials for Enterprise Message Service transport. While using tibspmpassword, do not start a password with the following special characters: # (pound or hash sign) or (exclamation sign).</p> <p>This folder also has various TRA configuration files, corresponding to the set of executables mentioned in the earlier column. It also has convenience scripts (setspm4ems.*) to set up Enterprise Message Service artifacts for Service Performance Manager.</p>
TIBCO_HOME/spm/<version>/config	Contains the configuration files required by the Server, example, and Logger.	This folder contains log4j, spm, spmdashboard, schema files.
TIBCO_HOME/spm/<version>/apidocs	Contains the APIs	api — Contains JavaDoc API for all Service Performance Manager client APIs.
TIBCO_HOME/spm/<version>/examples	Contains api, and probes, and schemas subfolders.	<p>api — Contains Java example code that executes as tibspmexamples on how to use client APIs, send facts, write queries, and so on.</p> <p>probes — Bundles some sample probes (source code and compiled library JAR).</p>

Directory	Description	Contents
TIBCO_HOME/spm/<version>/lib	Contains all the Service Performance Manager component libraries	
TIBCO_HOME/spm/<version>/logs	Default folder for dashboard and server logs	This is the default folder where Service Performance Manager logs are generated: spmdashboard.log and spm.log
TIBCO_HOME/spm/<version>/setup	Contains Service Performance Manager Post Install - automated setup script	
TIBCO_HOME/spm/<version>/spmdashboard	Contains Service Performance Manager Web Application archive (spmdashboard.war) and some scripts for monitoring dashboard data. If you do not wish to use the bundled Tomcat Web Container, deploy this WAR file in some other web container.	spmdashboard.war startspmdashboard.bat stopspmdashboard.bat
TIBCO_HOME/spm/<version>/spmdashboard/tomcat	Contains the Tomcat web container	
TIBCO_HOME/spm/<version>/spmdashboard/tomcat/logs	Contains the log files for the Tomcat web container	
TIBCO_HOME/studio	Contains files related to TIBCO Business Studio.	
TIBCO_HOME/tct	Contains files related to TIBCO Configuration Tool.	
TIBCO_HOME/tibcohost		
TIBCO_HOME/tibcojre64	Contains files used by JRE.	
TIBCO_HOME/tools	Contains some tools and scripts such as the Universal Installer.	./lib ./scripts ./universal_installer ./wrapper

# Configuration

---

When you complete the installation, the installer prompts you to run the TIBCO Configuration Tool to configure the product. You can also choose to configure the product at a later time by launching the tool from `TIBCO_HOME/tct/1.6` or `TIBCO_HOME/amx/<version>/bin`.

The tool displays a list of wizards for products installed in the *TIBCO\_HOME* directory. Available options depend on the products installed in the *TIBCO\_HOME* directory. Configuration tasks for TIBCO ActiveMatrix Service Grid include creating runtime objects such as a TIBCO Host instance or an Administrator server.

## Configuration Setup and Overview

Use TIBCO Configuration Tool to specify the properties of the ActiveMatrix Administrator servers and TIBCO Host instances and also properties of third-party drivers you want to add to the ActiveMatrix Administrator servers.

You can run TIBCO Configuration Tool in the GUI mode, console mode, silent mode, or script mode.



Silent mode and script mode are for advanced users.

- In the GUI mode, the tool prompts for configuration information with a set of wizards.
- In the console mode, the tool prompts for configuration information on the command line.
- In the silent mode, you generate a configuration file by running a wizard in the GUI or console mode and responding to the prompts. Edit the configuration file, and then run the tool without user input.
- In the script mode, run a wizard in the GUI mode or console mode and explicitly save the configuration file, or edit one of the sample configurations. You then execute an Ant build from the command window of the folder in which your configuration is located.

## Networking

Before you start configuration, check whether the default ports that TIBCO Configuration Tool uses are available. You must also decide whether you want to use SSL, and might have to set up keystores and trust stores.

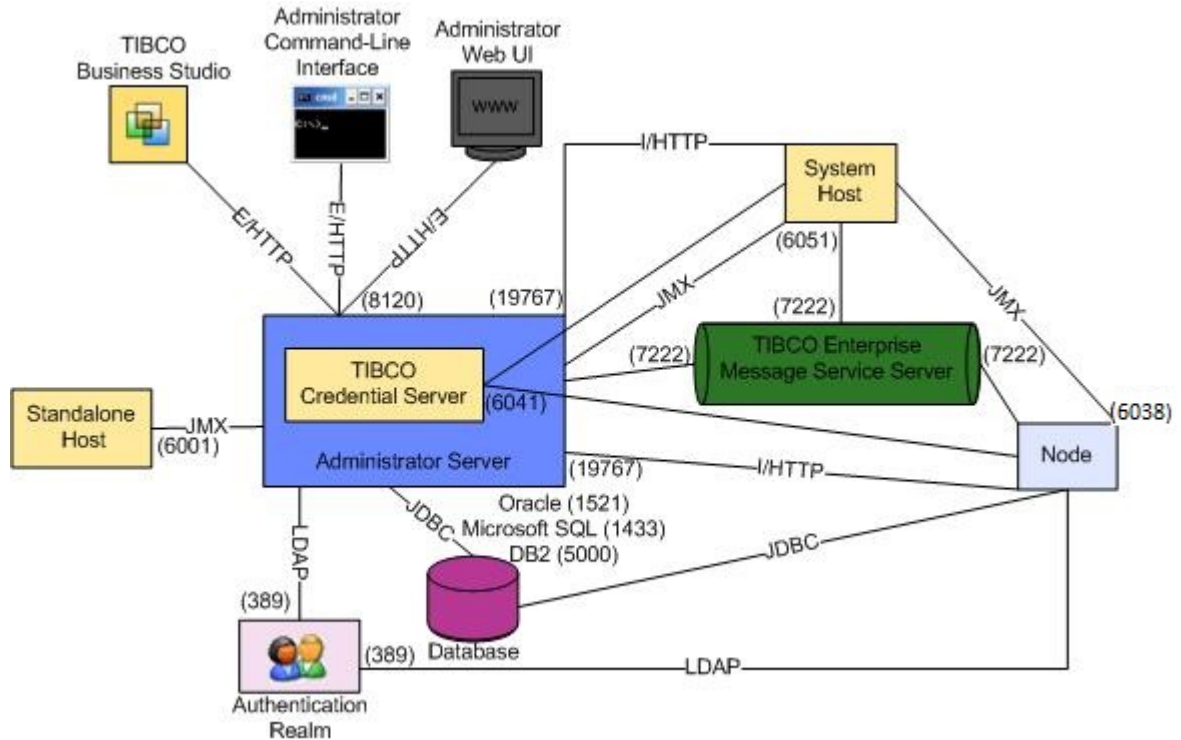
### Default Ports

The default ports in an ActiveMatrix environment must be available before you can start configuration with the default values. You can specify a different port during configuration, or change the ports explicitly later.

[Default Ports](#), [TIBCO ActiveMatrix Runtime Object Default Ports](#), and [Server Default Ports](#) summarize the default values of the ports configured in TIBCO Configuration Tool. You can change the defaults in TIBCO Configuration Tool wizards. For information on how to change the ports after you have created runtime objects with TIBCO Configuration Tool, see the *TIBCO ActiveMatrix Service Grid Administration* guide.



## Default Ports



## TIBCO ActiveMatrix Runtime Object Default Ports

Runtime Object	Default Port
SystemHost TIBCO Host instance management	6051
Standalone TIBCO Host instance management	6001
System node management	6021
Development node management	6038
TIBCO ActiveMatrix Administrator external HTTP	8120
TIBCO ActiveMatrix Administrator internal HTTP	19767
TIBCO Credential Server	6041

## Server Default Ports

Server	Default Port
Enterprise Message Service	7222 or 7243 (SSL)
Database	Oracle 1521 Microsoft SQL 1433 IBM DB2 5000

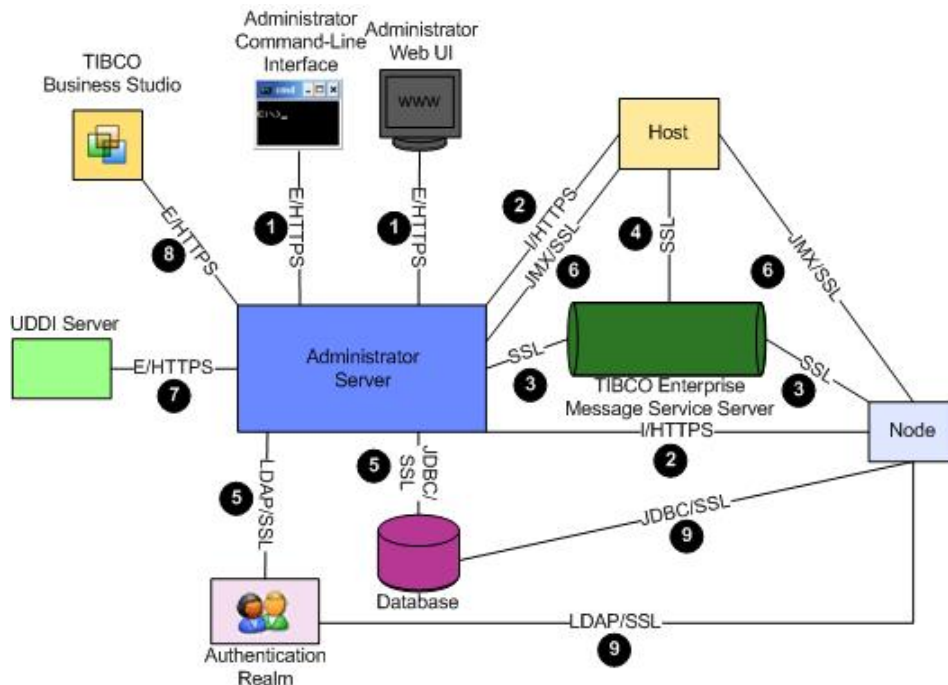
Server	Default Port
LDAP	389

## Secure Communication Channels

The ActiveMatrix platform is partitioned across many components. You can secure the corresponding communication channels during the initial configuration or later.

ActiveMatrix components communicate with each other and with third-party applications over several communication protocols. [Communication Channels](#) illustrates the components and communication protocols.

### Communication Channels



By default, the communication channels are not secure. To secure them, you can configure the channels to use the Secure Sockets Layer (SSL) protocol. SSL is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks.

An SSL client and server negotiate a connection by using a handshaking procedure. During this handshake, the client and server agree on various parameters to establish the connection's security, as follows:

1. A client requests a secure connection from an SSL-enabled server requesting a secure connection.
2. The server sends back its identification in the form of a digital certificate.

The certificate usually contains the server name, the trusted certificate authority (CA), and the server's public encryption key.

You can specify the SSL configuration of the communication channels at different times in the life cycle of a deployment. The table below lists how to perform the initial SSL configuration and how to upgrade, downgrade, and change the configuration of each channel. The Key column in the table refers to the numbers in the diagram above.

### SSL Configuration Summary

Key	Channel	Initial Configuration	Upgrade, Downgrade, or Change Configuration
1	Administrator server (external HTTP port) - web and CLI clients	When creating the Administrator server in TIBCO Configuration Tool.	Upgrade or downgrade: Administrator CLI Change SSL configuration: Administrator CLI
2	Administrator server (internal HTTP port) - hosts and nodes	When creating the Administrator server in TIBCO Configuration Tool.	Upgrade or downgrade: Administrator web UI or CLI Change SSL configuration: Administrator web UI or CLI
3	Administrator server - Enterprise Message Service server (Notification Server and Messaging Bus)	When creating the Administrator server in TIBCO Configuration Tool.	Upgrade or downgrade: Administrator web UI or CLI Change SSL configuration: Administrator web UI or CLI
4	TIBCO Host instance - TIBCO Enterprise Message Service	When creating the Administrator server or TIBCO Host instance in TIBCO Configuration Tool.	Upgrade or downgrade: Administrator CLI Change SSL configuration: Administrator CLI
5	Administrator server - external database and LDAP servers	When creating the Administrator server in TIBCO Configuration Tool.	Change SSL configuration: Administrator CLI
6	Administrator server - hosts and nodes (management)	When creating Administrator in TIBCO Configuration Tool.	Upgrade: Administrator web UI or CLI Change SSL configuration: Administrator CLI
7	Administrator - UDDI server	Manually import the UDDI server certificate into the Administrator server trust store using keytool.  Enable secure communication in Administrator web UI or CLI.	Same procedure as initial configuration

Key	Channel	Initial Configuration	Upgrade, Downgrade, or Change Configuration
8	Administrator server (external HTTP port) - TIBCO Business Studio	Administrator - When creating Administrator server in TIBCO Configuration Tool. TIBCO Business Studio - When you connect to Administrator.	Administrator Upgrade or downgrade: Administrator CLI Change SSL configuration: Administrator CLI
9	Resource instances (JDBC, JMS, SMTP, LDAP, HTTP) - external servers	Administrator web UI or CLI	Administrator web UI or CLI

## Keystores

If you set up your environment for SSL, you have to set up a keystore. As part of the process, you configure a keystore provider.

SSL uses keys and certificates when it establishes the secure connection. A *keystore* is a database of keys and certificates. A keystore password is required to access or modify the keystore.

Access to keystores is provided by a Keystore Provider resource instance. Keystores can be stored internally in Administrator or externally.

### ActiveMatrix Administrator Default Keystore

In TIBCO ActiveMatrix access to keystores is provided by a Keystore Provider resource instance. When you create an Administrator server, TIBCO ActiveMatrix includes a default keystore provider resource template named `tibco.admin.default.keystore` that references the default keystore `CONFIG_HOME/admin/amxadmin/shared/repo/trunk/artifacts/keystore/admin_default_keystore.jceks`.

### Keystore Entries

A keystore has two types of entries:

- Private key - holds a cryptographic private key, which is optionally stored in a protected format to prevent unauthorized access. The private key is accompanied by a certificate chain for the corresponding public key. Private keys and certificate chains are used by a given entity for self-authentication.
- Trusted certificate - contains a single public key certificate. It is called a trusted certificate because the keystore owner trusts that the public key in the certificate belongs to the identity identified by the subject (owner) of the certificate. This type of entry can be used to authenticate other parties.

Certificates of trusted entities are typically imported into a keystore as trusted certificates.

### Keystore Entries and Aliases

Each entry in a keystore is identified by an *alias*. In the case of private keys and their associated certificate chains, these aliases distinguish among the different ways in which the entity may authenticate itself. For example, the entity may authenticate itself using different certificate authorities, or using different public key algorithms. An alias might be named after the role in which the keystore owner uses the associated key, or might identify the purpose of the key.

## Keystore Passwords and Private Key Passwords

The private keys in a keystore are encrypted with a keystore password, which should be several words long.

You can also protect each private key with its individual password, which may or may not be the same as the keystore password.



If a password is lost, the associated keys cannot be recovered.

## Trust Stores

A trust store is a keystore that contains trusted certificates. Each time you configure an external server connection for SSL, you create and configure a trust store for that connection.

You can create a trust store by using certificates imported from trusted servers or by uploading a keystore file.

## Creating a Trust Store Keystore

You can create a trust store with `keytool` if you have a trusted public certificate.

### Procedure

1. Acquire the public certificate for your server or the root CA certificate authority that signed the certificate.

A root CA is an entity like VeriSign that digitally signs your certificate. The certificate will be in a file with a special extension such as `.pem` extension.

2. Use the JDK `keytool` utility to create a keystore containing the certificate from [step 1](#).

```
JAVA_HOME\bin\keytool -import -v -trustcacerts -alias MyCert
-file server.cer -keystore MyTrustStore.jks -keypass secret -storepass
keystorePassword
```

Record the values of the `keytool` options because you must supply them when you upload the trust store keystore into TIBCO Configuration Tool or Administrator.

## Configuring a Trust Store

To configure a trust store, you can either upload certificates and have TIBCO Configuration Tool create the trust store, or you upload a keystore file that contains certificates.

If you configure a trust store for use with an SSL-enabled Microsoft SQL Server, you must upload a keystore. For Microsoft SQL databases, the **Configure a Trust Store** button does not work.

### Procedure

1. Choose the method for configuring the trust store and follow the appropriate procedure.

Method	Description
Import	<ol style="list-style-type: none"> <li>1. Click <b>Create a Trust Store</b>.</li> <li>2. Specify a password to protect the keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>3. In the Trust Selected Certifications area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>

Method	Description
	A keystore file is created containing the selected certificates and the Keystore Location, Keystore Type, and Keystore Password fields are filled in with the keystore information.
<b>Upload</b>	<ol style="list-style-type: none"> <li>1. <a href="#">Create a keystore</a> containing the certificates from the trusted server.</li> <li>2. Click <b>Browse</b> and navigate to the location of the keystore you created.</li> <li>3. Click the keystore and click <b>Open</b>. The wizard fills in the Keystore Location field.</li> <li>4. From the Keystore Type drop-down list, select the keystore type.</li> <li>5. Type the keystore password.</li> </ol>

2. Click **Test Connection** to verify that the keystore enables an SSL connection.

## IPv6 Support

If an object has a property that can contain an IP address, the address is usually set to the unspecified IP address (0.0.0.0). That means the object listens on IPv4 and IPv6 addresses. By default clients use the IPv4 address. You can override this behavior so that clients use the IPv6 address.

### Prerequisites

Before using an IPv6 supported network, perform the following tasks:

1. Complete all the network configuration changes required for network traffic routing.
2. Enable all physical machines participating in the installation topology for IPv4 and IPv6 addressing in dual-stack IP implementations.
3. Configure the names of all machines to resolve to at least one IPv4 or IPv6 address.
4. Configure clients to communicate with the servers in one of the following ways:
  - a. Use explicit IPv4 or IPv6 addresses.
  - b. Use the addresses returned by the address translation mechanism (DNS or local host files) performed on the machine name.

### IPv6 Address Support

IPv6 addresses are supported by machine names and URLs in the following tools and objects:

- TIBCO Configuration Tool
- Administrator and TIBCO Business Studio wizards and CLI property files
- Components that use dynamic wiring
- Resource templates

### IPv6 Address Representation

IPv6 address representation is described in the [IPv6 Addressing Architecture](#) and [Format for Literal IPv6 Addressing in URLs](#) specifications, and summarized in [IPv6 Address Representation](#).

## IPv6 Address Representation

Address Type	Representation
All	<p>Eight fields of four hexadecimal digits, where each field is separated by a colon. If the field is non-zero there must be at least one digit. For example, 2001:db8:1234:ffff:4354:45ab:3455:ab45. You can apply the following shortening procedures:</p> <ul style="list-style-type: none"> <li>• Omit leading zeros in a field. For example, :00db: can be represented as :db:.</li> <li>• Replace one or more consecutive fields of zeros and separators (:0:0:0:0:) with a single empty field (::). For example, 2001:db8:0:0:0:0:3455:ab45 can be represented as 2001:db8::3455:ab45.</li> </ul>
Localhost or loopback	0:0:0:0:0:0:0:1 or ::1.
Unspecified	0:0:0:0:0:0:0:0 or ::. This address is equivalent to the unspecified IPv4 address 0.0.0.0.
Embedded in a URL	Enclose the address in square brackets ([ ]). For example, the URL of an Administrator server running on a machine at the address FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 is http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:8120/amxadministrator.

### IP Address Use and Resolution

The default configuration of the Administrator server network adapter is the unspecified IP address (0.0.0.0), which means that it listens on IPv4 and IPv6 addresses. When clients access the Administrator server by machine name, the name lookup resolves to both addresses. By default, Administrator clients use the IPv4 address. To override this behavior and use the IPv6 address, set the value of the JVM system property `java.net.preferIPv6Addresses` to `true` in the Administrator Node. The Managing Nodes section in *Administration Guide* explains how to set a JVM property for a Node.

## TIBCO Configuration Tool Requirements

You can run TIBCO Configuration Tool right after installation or at a later time. To run the tool successfully, you must first make sure your system meets the requirements.

Each product installation has a set of requirements. TIBCO Configuration Tool has additional requirements.

- You must have access to a running instance of TIBCO Enterprise Message Service server. See [Enterprise Messaging Server Requirements](#).
- If you do not have administrator privileges for the Enterprise Message Service server, you must set up Enterprise Message Service for a non-administrator user. See [Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users](#).
- If you want to secure communication with SSL, you must perform additional setup. See [Secure Communication Channels](#) for background and setup information and [SSL Requirements](#) for specific requirements.



See the Readme file for requirements.



## Enterprise Messaging Server Requirements

To run successfully, TIBCO Configuration Tool must have access to a TIBCO Enterprise Message Service that meets certain requirements.

A TIBCO Enterprise Message Service server acts as a notification server for the ActiveMatrix Administrator servers and TIBCO Host instances within an enterprise. The enterprise is defined by the enterprise name and the TIBCO Enterprise Message Service server that you specify when you run one of the configuration wizards. Ensure that the following requirements and prerequisites are satisfied:

- Each enterprise must use a different TIBCO Enterprise Message Service server.
- The TIBCO Enterprise Message Service server must be running before you run the Create TIBCO ActiveMatrix Administrator Server and Create TIBCO Host Instance wizards or create these components in the console mode or silent mode.
- If you manually start the TIBCO Enterprise Message Service server, make sure you use the same configuration files as the Windows service. Use the following command:  

```
TIBCO_HOME/ems/version number/bin/tibemspd -config EMS_CONFIG_HOME/tibco/cfgmgmt/ems/data/tibemspd.conf
```

 where *EMS\_CONFIG\_HOME* is the configuration folder for TIBCO Enterprise Message Service.
- The clocks of machines within the same enterprise must be synchronized to within 30 minutes. You can run an NTP synchronization daemon on each machine to achieve synchronization.
- If you do not have administrator privileges for TIBCO Enterprise Message Service, you can request privileges or configure the service for a non-admin user from the TIBCO Enterprise Message Service server console. See [Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users](#).
- The connection factory details are specified in the `factories.conf` file of TIBCO Enterprise Message Service.
- Permissions for creating dynamic queues have been set in the `queues.conf` file of TIBCO Enterprise Message Service.
- TIBCO ActiveMatrix platform supports TIBCO Enterprise Message Service configured with a JSON configuration file and `.conf` file. Refer to the *TIBCO Enterprise Message Service™ User's Guide* for more details.

## SSL Requirements

By default, ActiveMatrix runs with SSL disabled. You can enable SSL for individual connections or for all connections in your environment.

See [Secure Communication Channels](#) for information on setting up SSL. If you intend to enable SSL, ensure the following prerequisites are satisfied.

- **TIBCO Enterprise Message Service server** - The TIBCO Enterprise Message Service server must be enabled with SSL and configured with a certificate file that contains both the server and issuer certificates before you run the Create TIBCO Administrator server and Create TIBCO Host Instance wizards or before you create these components in console mode or silent mode.

This release of ActiveMatrix ships with Java 8. As a result, you must either use an Enterprise Message Service server 6.3 or a later version or use a stream cipher.

- **Database and LDAP Servers** - Database and LDAP servers must be enabled with SSL before you run the Create TIBCO Administrator Server wizard or before you create these components in the console mode or silent mode.

See [Secure Communication Channels](#).



## Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users

Configuration of TIBCO ActiveMatrix runtime objects and services is easiest if you have administrative privileges on the TIBCO Enterprise Message Service server you want to use. If you do not have administrative privileges, you can set up the TIBCO Enterprise Message Service server to configure Enterprise Message Service servers for non-admin users.

If you want to configure TIBCO ActiveMatrix runtime objects and services, and you do not have administrator privileges on the TIBCO Enterprise Message Service server you want to use, you can configure the TIBCO Enterprise Message Service server to configure Enterprise Message Service servers for non-admin users. The following steps list the most restrictive permissions necessary.

### Procedure

1. In the TIBCO Enterprise Message Service server console, set permissions for the Administrator server users. In the following commands, replace *username* and *password* with the username and password values appropriate for each bus.

- **Messaging Bus**

```
delete queue >
delete topic >
create user username "Description of the user" password=password
create queue AMX_SV.>
grant queue AMX_SV.> user=username create, delete, modify, send, receive
```

- **Notification Bus**

```
delete queue >
delete topic >
create user username "Description of the user" password=password
create topic EMSGMS.>
grant topic EMSGMS.> user=username create, modify, subscribe, publish
grant topic $sys.monitor.connection.* user=username subscribe
grant admin user=username view-connection,view-server
create topic AMX_MGMT.>
grant topic AMX_MGMT.> user=username create, modify, subscribe, publish
create queue AMX_MGMT.>
grant queue AMX_MGMT.> user=username create, delete, modify, send, receive
```

- **Management Bus**

```
delete queue >
delete topic >
create user username "Description of the user" password=password
create queue com.tibco.amf.admin.deploymentServerQueue.>
grant queue com.tibco.amf.admin.deploymentServerQueue.> user=username
create, delete, send, receive
```

- **Logging and Payload Buses**

```
delete queue >
delete topic >
create user username "Description of the user" password=password
create queue cl_logservice_queue.physical
create queue cl_payload_queue.physical
grant queue cl_logservice_queue.physical user=username send, receive
grant queue cl_payload_queue.physical user=username send, receive
create jndiname cl_logservice_queue queue cl_logservice_queue.physical
create jndiname cl_payload_queue queue cl_payload_queue.physical
```

- **Monitoring Bus**

```
delete queue >
delete topic >
create user username "Description of the user" password=password
create queue amx.governance.stats
grant queue amx.governance.stats user=username send, receive
create queue amx.governance.internal.stats
grant queue amx.governance.internal.stats user=username send, receive
```

2. If you intend to manually separate notification, management, and messaging buses, group their constraints first.

The Notification, Management, and Messaging buses are initially grouped together as are the Monitoring, Logging, and Payload buses.

- **Messaging, Notification, and Management Buses**

```
delete queue >
delete topic >
create user username "Description of the user" password=password
create queue AMX_SV.>
grant queue AMX_SV.> user=username create, delete, modify, send, receive
create topic EMSGMS.>
grant topic EMSGMS.> user=username create, modify, subscribe, publish
grant topic $sys.monitor.connection.* user=username subscribe
create queue com.tibco.amf.admin.deploymentServerQueue.>
grant admin user=username view-connection,view-server
grant queue com.tibco.amf.admin.deploymentServerQueue.> user=username
create, delete, send, receive

create topic AMX_MGMT.>
grant topic AMX_MGMT.> user=username create, modify, subscribe, publish

create queue AMX_MGMT.>
grant queue AMX_MGMT.> user=username create, delete, modify, send, receive
```

- **Monitoring, Logging, and Payload Buses**

```
delete queue >
delete topic >
create user username "Description of the user" password=password
create queue cl_logservice_queue.physical
create queue cl_payload_queue.physical
create queue amx.governance.stats
create queue amx.governance.internal.stats
grant queue cl_logservice_queue.physical user=username send, receive
grant queue cl_payload_queue.physical user=username send, receive
grant queue amx.governance.stats user=username send, receive
grant queue amx.governance.internal.stats user=username send, receive
create jndiname cl_logservice_queue queue cl_logservice_queue.physical
create jndiname cl_payload_queue queue cl_payload_queue.physical

create queue AMX_SV.>
grant queue AMX_SV.> user=username create, delete, modify, send, receive
create topic EMSGMS.>
grant topic EMSGMS.> user=username create, modify, subscribe, publish
```

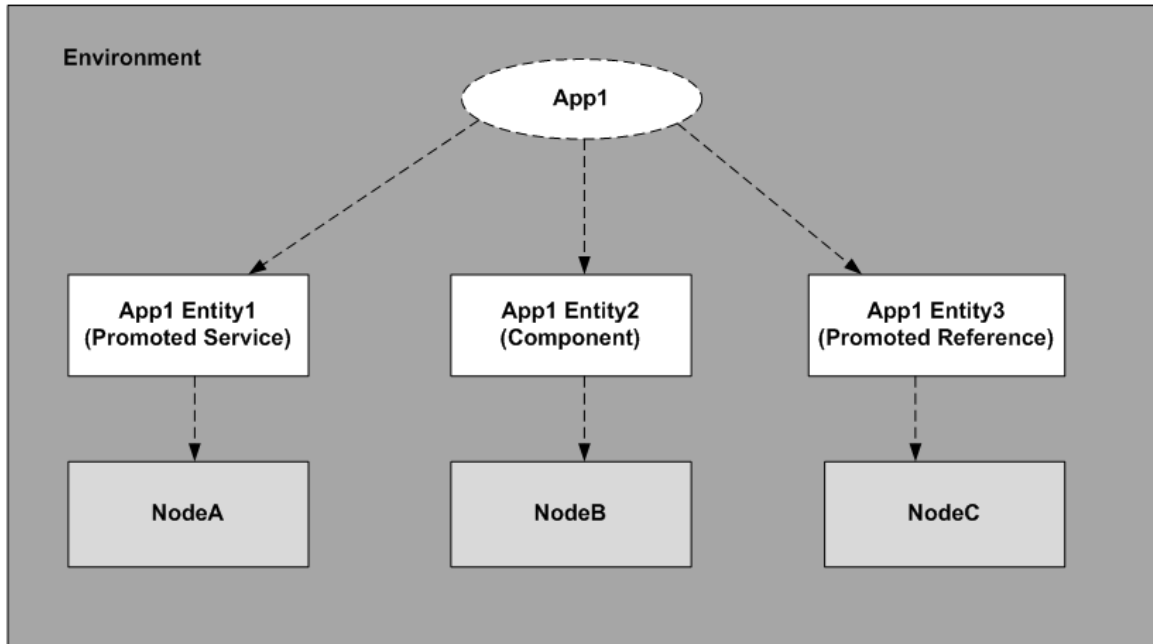
3. Configure and create the Administrator server and TIBCO Host instances as described in [Create TIBCO ActiveMatrix Administrator Server](#) and [TIBCO Host Instance](#).

## Determining Whether an Enterprise Needs a Messaging Bus

A messaging bus is required only when distributing an application across multiple nodes. As an example, the following figures depict a setup with multiple nodes and help you identify scenarios where a messaging bus might or might not be required.

The following figure shows a scenario where a messaging bus is required.

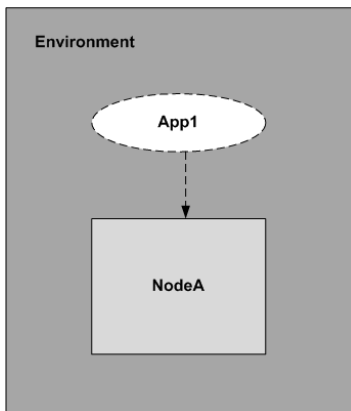
### *Messaging Bus Required - Application Entities Deployed Across Multiple Nodes*



In the above figure, consider that different entities of a single application (**App1**) need to be deployed across different nodes. **Entity1** (a promoted service) needs to be deployed to **NodeA**, **Entity2** (a component) needs to be deployed to **NodeB**, and **Entity3** (a promoted reference) needs to be deployed to **NodeC**. A messaging bus is required in this case.

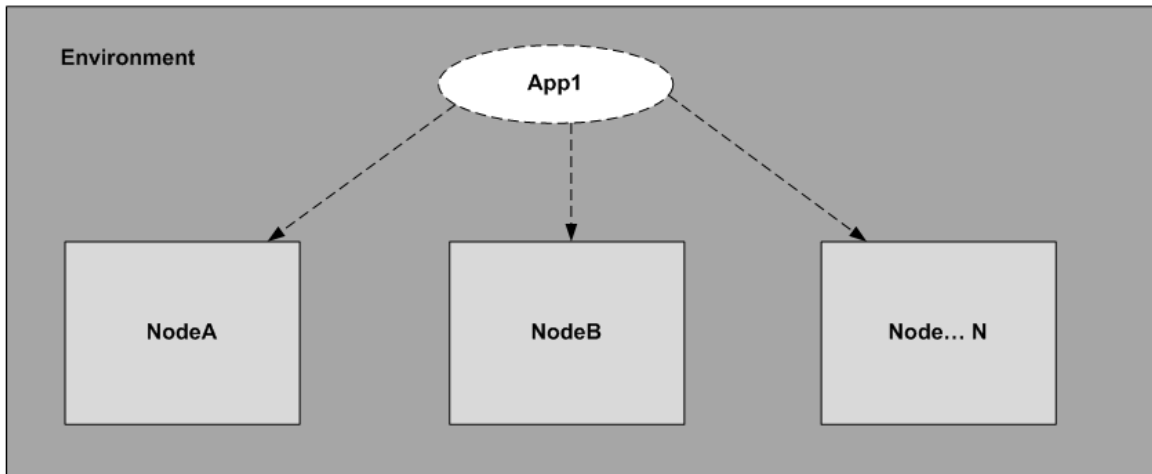
The following figures show scenarios where a messaging bus is not required.

### *Messaging Bus Not Required - Single Application Deployed to Single Node*



In the above figure, consider that a single application (**App1**) needs to be deployed to a single node (**NodeA**). A messaging bus is not required in this case.

*Messaging Bus Not Required - Single Application Deployed Across All Nodes And Each Node is Distributed with All Entities of the Application*



In the above figure, consider that a single application (App1) needs to be deployed across all the nodes (NodeA, NodeB, Node . . . N) in the environment. Consider that all the components of App1 run on all the nodes all the time and none of the application entities (such as component, service, binding, reference, and so on) are distributed across multiple nodes. A messaging bus is not required in this case. For scenarios like these, you can deploy an application even when the messaging bus is down or not available.

### Creating an Enterprise With or Without a Messaging Bus

Using TIBCO Configuration Tool (TCT), you can create an enterprise that:

- Does not use the messaging bus.

In this case:

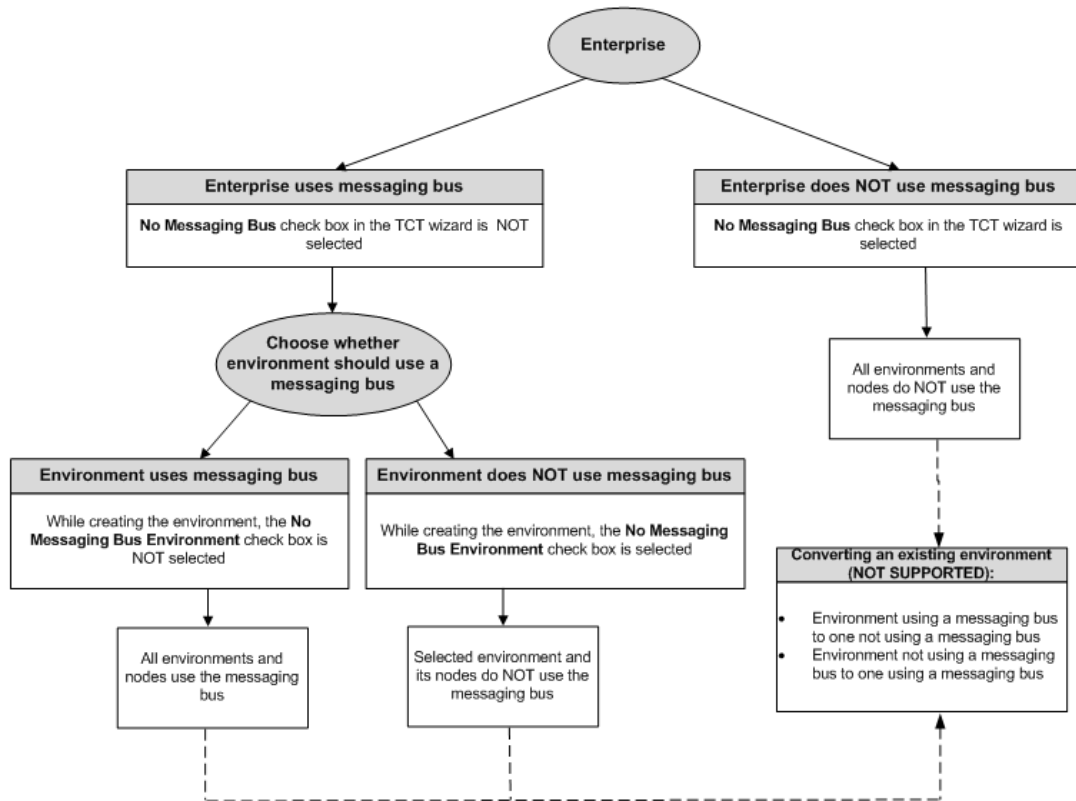
- All the environments in the enterprise do not use the messaging bus.
- All the nodes in the enterprise do not use the messaging bus.

For more information on how to create an enterprise that does not use the messaging bus using the TCT wizard, see [Administrator Server Notification and Messaging Bus Server](#).

- Uses a messaging bus.

If you create an enterprise that uses the messaging bus, after the enterprise is created, you can use TIBCO ActiveMatrix Administrator to decide and configure whether an environment should use a messaging bus or not. For more information on how to configure messaging bus settings related to an environment, see *TIBCO ActiveMatrix Service Grid Administration Guide*.

The following illustration summarizes the messaging bus configuration:



## Running TIBCO Configuration Tool

You can run TIBCO Configuration Tool using the GUI, console, or silent mode.

### Running TIBCO Configuration Tool in GUI Mode

When you run TIBCO Configuration Tool in the GUI mode, you are prompted to select a configuration wizard. The wizard prompts you for information about that component.

#### Prerequisites

Make sure your system meets all requirements. See [TIBCO Configuration Tool Requirements](#).

#### Procedure

1. Execute `TIBCO_HOME/amx/<version>/bin/TIBCOConfigurationTool`. Alternatively, you can also execute `TIBCO_HOME/tct/<version>/bin/TIBCOConfigurationTool`. The TIBCO Configuration Folder dialog is displayed. The TIBCO configuration folder stores configuration data generated by TIBCO products. Configuration data can include sample scripts, session data, configured binaries, logs, and so on. The configuration folder is referred to as `CONFIG_HOME`.
2. Accept the default folder for `CONFIG_HOME`, type a folder name, or click **Browse** to select a folder, and click **OK**.
3. TIBCO Configuration Tool displays with links to the configuration wizards. The wizards the tool presents depend on the products currently installed in your environment.

Wizard	Function
<a href="#">Create Express Developer Environment</a>	Specify the name and server properties of an ActiveMatrix Administrator server and the machine name, port, and credentials of the TIBCO Enterprise Message Service server used by the Administrator server. The TIBCO Host instance named SystemHost and the SystemNode node that runs ActiveMatrix Administrator server are started. The rest of the configuration properties are set to the default values described in <a href="#">Create TIBCO ActiveMatrix Administrator Server</a> .
<a href="#">Create TIBCO ActiveMatrix Administrator Server</a>	<ul style="list-style-type: none"> <li>Specify the properties of an ActiveMatrix Administrator server and optionally create the server. The SystemHost TIBCO Host instance and the SystemNode node that runs ActiveMatrix Administrator server are started.</li> <li>Optionally specify a development environment and node and start the node.</li> <li>Specify the properties of monitoring, logging, and payload services running on SystemNode and optionally deploy the monitoring and logging services.</li> <li>Specify the database that serves as a persistent store for ActiveMatrix Administrator server and the monitoring, logging, and payload services.</li> <li>Optionally deploy sample applications and object groups to get started with a Hello World application and object groups to apply policies on.</li> </ul>
<a href="#">Create TIBCO ActiveMatrix Policy Director Governance Administrator Server</a>	Configure a TIBCO ActiveMatrix Policy Director Governance Administration server. You can create a new server or configure an existing Administration server as a TIBCO ActiveMatrix Policy Director Governance server.
<a href="#">Create TIBCO ActiveMatrix Policy Director Governance Proxy Host</a>	Configure a TIBCO ActiveMatrix Policy Director Governance proxy host.
<a href="#">Create TIBCO Host Instance</a>	Specify the communication and management properties of a standalone TIBCO Host instance and optionally create and launch the TIBCO Host instance.
<a href="#">Configure Third-Party Driver</a>	Package and install third-party client driver libraries that implement APIs such as JDBC and JMS into the ActiveMatrix Administrator server software repository.
<a href="#">Edit ActiveMatrix Administrator Server Configuration</a>	Edit an existing ActiveMatrix Administrator server configuration.

Wizard	Function
<a href="#">Replicate TIBCO ActiveMatrix Administrator Server</a>	Configure a Replica server for a clustered environment.
<a href="#">Upgrade or Downgrade TIBCO ActiveMatrix</a>	Allows you to upgrade the existing ActiveMatrix Service Grid enterprise to the current release. It also allows you to downgrade from the current release of ActiveMatrix Service Grid to an older release.
<a href="#">Update JRE</a>	Update the TIBCO_HOME (and all CONFIG_HOMEs using the TIBCO_HOME) to use the specified JRE version.
<a href="#">Configure Service Performance Manager Server</a>	Configure the Service Performance Manager server.
<a href="#">Configure TIBCO ActiveMatrix SPM Dashboard</a>	Configure the TIBCO ActiveMatrix SPM dashboard.



TIBCO Hawk ActiveMatrix® Plug-in gets installed with the following three wizards:

- Create Express Developer Environment
- Create TIBCO ActiveMatrix Administrator Server
- Create TIBCO Host Instance

For further information, see *TIBCO Hawk ActiveMatrix® Plug-in User's Guide*.

4. Click a wizard link and follow the prompts.  
The wizard reference, also available as online help, can help guide your decisions.
5. Optionally, select the **Configure to Secure All Communication with SSL** checkbox.  
When you enable SSL, the wizards containing communication channels display the SSL configuration fields. For information on the supported communication channels, see [Secure Communication Channels](#).
6. Optionally, click **Load** to load the values saved from a previous configuration session. See [Saving a TIBCO Configuration Tool Configuration](#).
7. On any screen, click **Finish** to accept the default values for all the configuration properties and move to the Summary screen.
8. Review the Summary screen and select or clear check boxes for wizard actions.
9. Click **Configure**.

## Running TIBCO Configuration Tool in Console Mode

You can run TIBCO Configuration Tool from the command prompt on the platform of your choice.

### Prerequisites

Make sure your system meets all requirements. See [TIBCO Configuration Tool Requirements](#).

You can run TIBCO Configuration Tool in the GUI mode, console mode, or silent mode. The mode you used for running the installer does not affect the mode in which you run TIBCO Configuration Tool.

### Procedure

1. In a console window, go to the `TIBCO_HOME\tct\version` directory and run the following command.

Platform	Description
Linux, UNIX	<code>TIBCOConfigurationTool -consoleMode</code>
Windows	<code>TIBCOConfigurationToolc.exe -consoleMode</code>



On Windows, the name ends with a c; do not type `TIBCOConfigurationTool -consoleMode`.

2. Select one of the configuration options and press **Enter**.
3. Type 1 or press **Enter** to configure all communications with SSL, or type N to continue.  
For information on the supported communication channels, see [Secure Communication Channels](#).
4. Follow the configuration tool prompts to set up your environment. After you review the pre-installation summary, type G to start the configuration process.  
When configuration completes, you can select a second configuration option or type q to quit.

## Running TIBCO Configuration Tool in Silent Mode

You can configure your system without user input by running TIBCO Configuration Tool in silent mode. You can supply parameters that specify which wizard you want to run, and you can specify which configuration file you want to use.

Before you run in the silent mode, you should run the tool in GUI mode to generate a configuration file (`build.properties`). You can then run in silent mode, pointing to the configuration file you generated.

Each `build.properties` file specifies the machine name and operating system. If you want to use that properties file to run in the silent mode on a different machine, potentially with a different operating system, you can edit the properties file. You might have to change the following values in the configuration file.

- Machine name (must be changed)
- ActiveMatrix installation location
- ActiveMatrix runtime configuration data location
- ActiveMatrix enterprise name
- Operating system (optional)



You must be an advanced user with an in-depth understanding of the configuration process to successfully run TIBCO Configuration Tool in the silent mode.

### Procedure

1. Run the tool in the GUI mode or in console mode to generate a properties file.  
`build.properties` file is stored in `CONFIG_HOME/tct/subfolder/date-time/scripts`.  
The name of *subfolder* depends on the wizard you run in the GUI or console mode.
2. Edit the `build.properties` file and customize the configuration. In most cases, you specify a different machine name, Administrator server, and so on.  
See [Using TIBCO Configuration Tool Scripts and Property Files](#).
3. Decide on the wizard you want to run.

Wizard	Wizard ID
Create TIBCO ActiveMatrix Administrator Server	<code>com.tibco.tct.admin</code>
Edit TIBCO ActiveMatrix Administrator Server	<code>com.tibco.tct.admin.editor</code>
Create Express Developer Environment	<code>com.tibco.tct.ede.admin</code>



Wizard	Wizard ID
Create TIBCO Host Instance	com.tibco.tct.tibcohost
Configure Third-Party Driver	com.tibco.tct.tpclshells
Replicate TIBCO ActiveMatrix Administrator Server	com.tibco.tct.admin.repliate
Create TIBCO ActiveMatrix Policy Director Governance Administrator Server	com.tibco.tct.pd
Create TIBCO ActiveMatrix Policy Director Governance Proxy Host	com.tibco.tct.pd.proxy
Upgrade or Downgrade TIBCO ActiveMatrix	com.tibco.tct.amx.upgrade.downgrade
Update JRE used by TIBCO ActiveMatrix	com.tibco.tct.update.jre
Configure TIBCO Service Performance Manager	com.tibco.tct.spm
Configure TIBCO ActiveMatrix SPM Dashboard	com.tibco.tct.amx.spm

4. From a console window, run TIBCO Configuration Tool in silent mode.

Platform	Command
Linux, UNIX	<code>TIBCOConfigurationTool -silentMode -wizard.id <i>wizard_id</i> -wizard.props <i>build_properties</i> [wizard.target <i>ant_target-name</i>]</code>
Windows	<code>TIBCOConfigurationToolc.exe -silentMode -wizard.id <i>wizard_id</i> -wizard.props <i>build_properties</i> [wizard.target <i>ant_target-name</i>]</code>

- *wizard\_id* can be one of the IDs listed in Step 3.
- *build\_properties* is a properties file for that wizard. You must customize most properties files before you run the wizard.
- *wizard\_target* is an optional parameter that is used to set a non-default build target. By default, the `build.xml` file of the wizard you invoke is used.

### Running in Silent Mode

```
TIBCOConfigurationToolc.exe -silentMode -wizard.id com.tibco.tct.admin -
wizard.props C:/build.properties -wizard.target admin-full-setup
```

## Using TIBCO Configuration Tool Scripts and Property Files

You save and edit property files that TIBCO Configuration Tool (TCT) generates, and perform configuration with those files by using an ANT script.



TCT-generated scripts, folder structure, and script properties of ActiveMatrix 3.4.0 and earlier versions of ActiveMatrix are different. You can load the saved scripts from earlier versions of ActiveMatrix in 3.4.0 TCT to update the configuration and save again.

When you run TCT, the tool creates property files and ANT build script files and stores them in the following location: `CONFIG_HOME/tct/<subfolder>/<date-time>/scripts`.

Each wizard creates its own sub folder under `CONFIG_HOME/tct`. Each sub folder contains the configuration scripts under the `TIMESTAMP` folder.

The following table lists the sub folder names created corresponding to each wizard.

Wizard	Sub Folder Name
Create TIBCO ActiveMatrix Administrator Server	admin
Edit TIBCO ActiveMatrix Administrator Server	admin.editor
Create Express Developer Environment	ede
Create TIBCO Host Instance	tibcohost
Configure Third-Party Driver	tpclshell
Create TIBCO ActiveMatrix Policy Director Governance Administrator Server	pd
Create TIBCO ActiveMatrix Policy Director Governance Proxy Host	pd.proxy
Replicate TIBCO ActiveMatrix Administrator Server	admin.replicate
Upgrade or Downgrade TIBCO ActiveMatrix	tct.upgrade.downgrade
Update JRE used by TIBCO ActiveMatrix	tct.update.jre
Configure TIBCO Service Performance Manager	tct.spm
Configure TIBCO ActiveMatrix SPM Dashboard	tct.amx.spm

Each wizard creates `build.xml`, `build.properties`, and a `templates` folder under the `scripts` directory.

- `build.xml`: Ant build file used to configure based on the saved data.
  - `build.properties`: Contains properties that are configured for the wizard.
  - `templates`: Contains wizard-specific template files that are used to generate the actual build and data files for use during configuration. These files are different for each wizard.
- A `tmp` folder is created when the build file is used. This `tmp` file contains the actual files created from the templates. These files are generated every time when configured through TIBCO Configuration Tool or Ant. If you change files in the `tmp` folder, they will be overwritten because the files are regenerated when you run the build file again.
  - The `build.properties` can be edited based on your needs. For example, when scripts are migrated to a new machine, all the machine-specific details and other relevant properties can be updated. Depending on the wizard type, you can select the properties that you want to edit.

Changing the name of `SystemEnvironment`, `SystemNode` and `SystemHost` is not supported. Changing the names will result in failure in case of some scenarios. For example, consider if you modify `SystemEnvironment`, `SystemNode`, and `SystemHost` to new names that is `DemoSystemEnvironment`, `DemoSystemNode`, and `DemoSystemHost` and then if you try to create TIBCO ActiveMatrix Administrator Server running TCT in silent mode, `deploy-mcr` target will fail. So it is not recommended to change the name of `SystemEnvironment`, `SystemNode` and `SystemHost`.

## Saving a TIBCO Configuration Tool Configuration

You can run a TIBCO Configuration Tool wizard in GUI mode to configure a component, and save those settings as a configuration file with an associated script.



A script that TIBCO Configuration Tool generates only works for the same minor version, even if you install other versions later. For example, if you generate a script in 3.2.x, that script uses the 3.2.x features and cannot use 3.3.x features even if 3.3.x is installed.

### Procedure

1. Run TIBCO Configuration Tool and select one of the wizards.
2. Specify configuration settings.
3. On the Session Scripts and Log Folder field of the Summary screen, accept the location of the configuration folder or click **Browse** to specify a new location.
4. Click **Save**.  
The configuration properties file and script is saved in the specified folder. The default folder is `CONFIG_HOME/data/tct/subfolder/date-time/scripts`, where
  - `CONFIG_HOME` is the folder you specify when you run the TIBCO Configuration Tool in one of the supported modes.
  - `subfolder` depends on the wizard you run.
5. Click **OK** to complete configuration.

## Reusing a TIBCO Configuration Tool Configuration

After you have saved a configuration file, you can run an Ant script to reuse the configuration.

### Prerequisites

Install and configure Ant on the target machine.

You can run TIBCO Configuration Tool and reuse the configuration on a different machine and operating system, if you edit the properties files to account for the following differences between the originating machine and the target machine.

- Machine name
- ActiveMatrix installation location
- ActiveMatrix runtime configuration data location
- ActiveMatrix enterprise name
- Operating system

Because all the property files specify the machine name, you must always replace the source machine name with the target machine name.



A script that TIBCO Configuration Tool generates only works for the same minor version, even if you install other versions later. For example, if you generate a script in 3.2.x, that script uses the 3.2.x features and cannot use 3.3.x features even if 3.3.x is installed. See [Modifying Scripts from Earlier Releases](#).

### Procedure

1. Make the required changes in the property files.

2. Open a command line window in the folder that has the properties file for the configuration you want to reuse. For example, open `CONFIG_HOME/tct/admin/<timestamp>/scripts`.
3. Run `ant [-logfile logfilename] -f build.xml`. This ANT command executes the default target in the `build.xml` file.

See [Using TIBCO Configuration Tool Scripts and Property Files](#).

## Configure Third-Party Driver Properties

You can configure third-party drivers by setting properties in a `build.properties` file and running a script.

To configure drivers, set the following properties in `tpclshells/build.properties`:

Property	Description
<code>shell.name</code>	Package name of the driver. See <a href="#">Shell Names and Versions</a> .
<code>shell.version</code>	Driver version.
<code>source.jar.folders</code>	Driver JAR file location.
<code>machine.model.location</code>	Machine model file.
<code>tibco.home</code>	ActiveMatrix installation location.

### Shell Names and Versions

Driver	Shell Name	Shell Version
Oracle Database 11g	com.tibco.tpcl.gen.oracle.jdbc	11.1.0.112100
Oracle 12c		12.1.100.121100
Oracle Database 12.1.0.x		12.1.100.121100
Oracle Database 12.2.0.1		12.2.0.1
Oracle Database 18c		18.3.0.001
Oracle Database 19c		19.3.0.001
Microsoft SQL Server 4.0.0	com.tibco.tpcl.gen.sqlserver.jdbc	4.0.0.400
Microsoft SQL Server 4.2.0		4.2.0.420
Microsoft SQL Server 6.0.0		6.0.0.600
Microsoft SQL Server 7.0.0		7.0.0.700
IBM DB2 4.12.55	com.tibco.tpcl.gen.db2.jdbc	4.12.55.4130
IBM DB2 4.19.66		4.19.66.41966

Driver	Shell Name	Shell Version
IBM DB2 4.24.92		4.24.92.42492
PostgreSQL 10.7.0	com.tibco.tpcl.gen.postgresql.jdbc	10.7.0.001
PostgreSQL 11.5.0		11.5.0.001
JMS Sonic	com.tibco.tpcl.gen.sonic.jms	6.1.0.620
JMS WebSphere	com.tibco.tpcl.gen.websphere.jms	7.0.0.001
SiteMinder Agent 6.0.0	com.tibco.tpcl.gen.siteminder	6.0.0.001
SiteMinder Agent 12.0.0		12.0.0.001

In most cases, you must modify the folder locations in the following properties.

- `source.jar.folders`
- `tibco.home`
- `machine.model.location`

Update the following properties to conform to target operating system path conventions:

Property	Description
<code>source.jar.folders</code>	Driver JAR file location.
<code>tibco.home</code>	Installation location.
<code>machine.model.location</code>	Machine model file.

## Create TIBCO Host Instance Properties

TIBCO Host Instance creation scripts are created under the `tibcohost` sub folder in `CONFIG_HOME/tct`.

You can modify the `build.properties` every time you want to create a new Host. Edit the properties listed in the table below and execute the `build.xml` to create the Host instance.

### Properties

To create a standalone TIBCO Host instance, update the following properties before running the script:

File Name	Property	Description
<code>build.properties</code>	<code>tibcohost.instance.name</code>	TIBCO Host instance name
	<code>tibcohost.jmx.host</code>	TIBCO Host instance machine name
	<code>tibcohost.jmx.port</code>	TIBCO Host instance management port

File Name	Property	Description
	admin.register.url	TIBCO Host instance management URL

### Enterprise Name

File Name	Property	Description
build.properties	tibcohost.enterprise.name	ActiveMatrix enterprise name

### Installation Location

Update the following property when the ActiveMatrix software is not installed in the default location.

File Name	Property	Description
build.properties	tibco.home	ActiveMatrix installation location.

### Configuration Folder Location

Update the following property when using a different configuration data folder location.

File Name	Property	Description
build.properties	tibco.config.mgmt.home	ActiveMatrix runtime state configuration location.



All the properties that contain a path must conform to the path conventions of the target operating system.

## Create ActiveMatrix Administrator Server Properties

ActiveMatrix Administrator Server creation scripts are created under admin sub folder in CONFIG\_HOME/tct.

You can modify the build.properties every time you want to create a new ActiveMatrix Administrator Server. Edit the properties listed in the table below and execute the build.xml to create the ActiveMatrix Administrator Server.

### Machine Name

Update the following properties with the correct machine name:

File Name	Property	Description
build.properties	serverconnsetting.host	Machine on which ActiveMatrix Administrator runs.
	serverconnsetting.port	ActiveMatrix Administrator Server Port number

File Name	Property	Description
	serverconnsetting.adminurl	ActiveMatrix Administrator server URL.

### Enterprise Name

Update the following property if the ActiveMatrix enterprise name has changed.

File Name	Property	Description
build.properties	admin.enterprise.name	ActiveMatrix enterprise name

### Installation Location

Update the following property when the ActiveMatrix software is installed in a different location.

File Name	Property	Description
build.properties	tibco.home	ActiveMatrix installation location.

### Configuration Folder Location

Update the following property when using a different configuration data folder location.

File Name	Property	Description
build.properties	tibco.config.mgmt.home	ActiveMatrix runtime state configuration location.



All the properties that contain a path must conform to the path conventions of the target operating system.

## Modifying Scripts from Earlier Releases

You cannot use ActiveMatrix 3.1.5 Configuration Tool scripts with ActiveMatrix 3.2.0 or later, but you can load a script from an earlier release.

### Procedure

- Find the script that you want to modify in your AMX 3.1.5 directory hierarchy.  
The location depends on the script. For example, look in `CONFIG_HOME\data\<wizard>\YYYY-MM-DD-hh-mm-ss\scripts`, for example, `CONFIG_HOME\data\tct\admin\YYYY-MM-DD-hh-mm-ss\scripts` for the Create Administrator Server wizard. To find `CONFIG_HOME`, look in for `tct.config.home` in the `TIBCOConfigurationTool.ini` file. This file is in `TIBCO_HOME\tct\version/`.
- When the wizard associated with ActiveMatrix 3.2.0 or later starts, click the **Load** button and browse to the ActiveMatrix 3.1.5 script you want to use.

## Configuration Tool Wizards and Screens

When you run TIBCO Configuration Tool in the GUI mode or in console mode, the system prompts you for information about the component or components you selected for configuration.

### Create Express Developer Environment

The Create Express Developer Environment wizard prompts for minimal configuration information and creates a host, a node, and an ActiveMatrix Administrator server running on the host. If you want more control over the configuration details, run the Create Administrator Server wizard.

When you select Create Express Developer Environment, a wizard prompts you for information about the Administrator server and the Enterprise Message Service to be used. When you complete the wizard, it creates an Administrator server, a host named SystemHost, and a node named SystemNode. At runtime, these components communicate using the Enterprise Message Service server you specify. The following table summarizes the information you need when running the wizard.

Component	Function	Options and Actions
<a href="#">Administrator Server</a>	Administers TIBCO ActiveMatrix applications and infrastructure.	Provide the name of the communication group within which status messages are exchanged and the name of the Administrator server. Provide communication properties for the Administrator server.
<a href="#">Notification and Messaging Bus Server</a>	Propagates status messages between hosts, nodes, and the ActiveMatrix Administrator server and messages between applications.	Provide configuration details for the Enterprise Message Service server.



## Administrator Server Configuration Details

The Administrator Server Configuration Details screen is used to specify the enterprise name and the name of the Administrator Server instance.

Field	Description
Enterprise Name	<p>Communication group for status messages that are sent between the Administrator server, the hosts that are bound to the server, and the nodes that are managed by those hosts.</p> <p>Default:</p> <ul style="list-style-type: none"> <li>amxadmin for ActiveMatrix Administrator</li> </ul> <p>The enterprise name specified here is displayed, by default, on the ActiveMatrix Administrator login banner as the default text, in default colors. The banner text and colors can be customized using the following properties in the <code>SystemNode.tra</code> file:</p> <ul style="list-style-type: none"> <li><code>java.property.com.tibco.admin.gui.login.screen.banner.text=&lt;Login Banner Text&gt;</code> Banner text for the Login screen.</li> <li><code>java.property.com.tibco.admin.gui.login.screen.banner.text.fontColor=&lt;RGB, HEX or HTML Color Name&gt;</code> Banner color for the Login screen.</li> <li><code>java.property.com.tibco.admin.gui.topPanel.banner.text=&lt;Navigation Banner Text&gt;</code> Banner text for the Navigation page.</li> </ul> <p>Both Banner texts, if not configured explicitly with System properties, currently display the name of the TIBCO Enterprise specified in the TIBCO Configuration Tool during Enterprise creation. A maximum of 80 characters of the Banner text are displayed, after which they are truncated and the complete text is displayed via a mouse-over HTML Tooltip.</p>
Server Name	<p>Name of the Administrator server.</p> <p>Default:</p> <ul style="list-style-type: none"> <li>instanceOne for ActiveMatrix Administrator</li> </ul>

## Administrator Server Notification and Messaging Bus Server

The Administrator Server Notification and Messaging Bus Server screen prompts you for the connection information for one or more TIBCO Enterprise Message Service server instances. The Notification and Messaging Bus servers in your express developer environment are then associated with that server.

You must have access to a running instance of TIBCO Enterprise Message Service Server before you can complete this screen. See [TIBCO Configuration Tool Requirements](#). If you intend to enable SSL communications, see [Secure Communication Channels](#).

Field	Description
Machine Name Port List	Comma-separated list of <i>machinename:port</i> addresses for a TIBCO Enterprise Message Service server.  Default: <i>machinename:port</i> , where <i>machinename</i> is the host on which TIBCO Configuration Tool is being executed and <i>port</i> is 7222. The default <i>machinename:port</i> is <code>tcp://hostname:7222</code> .
Username	Username for the TIBCO Enterprise Message Service server. The user must have administrator privileges in the TIBCO Enterprise Message Service server. If the user does not have administrator privileges, configure your TIBCO Enterprise Message Service server as described in <a href="#">Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users</a> .  Default: admin.
Password	Password for the TIBCO Enterprise Message Service user.  Default: None.
Test Connection	Click the <b>Test Connection</b> button to test the connection to TIBCO Enterprise Message Service server.

## Summary

With each TIBCO Configuration Tool wizard's summary screen, you can check the configuration that you specified and see the effects of that configuration. You can click **Back** to make changes, save the configuration for use by the silent installer, or click **Configure** to start the configuration. If you are using the console configuration tool, you can perform the same actions by typing single-letter commands.

Field	Description
Session Scripts and Log Folder	Folder containing the script configured in the wizard and the log file if the script is executed.
Administrator URL	If an Administrator server was configured in the wizard, a link to the URL of the Administrator server.
Actions	Actions that will be performed when the Configure button is clicked.
Products to Deploy	Product applications that will be deployed on the node if one has been configured.  If you did not deploy the logging and payload services when you created the Administrator server using the TIBCO Configuration Tool, see <code>TIBCO_HOME\administrator\version\scripts\logging\readme.txt</code> .
Save	Saves the configuration in the location specified in the Session Scripts and Log Folder field.
Configure	Saves the configuration in the location specified in the Session Scripts and Log Folder field and performs the actions specified in Actions and Products to Deploy.
Cancel	Returns to the wizard selector screen.

## Create TIBCO ActiveMatrix Administrator Server

The Create TIBCO ActiveMatrix Administrator Server wizard is used to configure many aspects of your server including the database, authentication method, monitoring, log service, and more.

You can review this wizard documentation before you start the configuration, to decide how you want to set up the server.



The wizard takes 15 minutes or more to complete depending on the configuration options.

### Database Requirements

When you run the wizard, specify a database for Administrator server and for several system services. If you are using an external database (and do not use HSQLDB as an external database), set up the external database before you run the wizard.

1. Package, install, and configure the database driver using the [Configure Third-Party Driver](#) wizard.
2. Configure the external database.

#### *Privileges Granted Based on the Database Type*

Database Type	Configuration Notes
Oracle	<p><b>Required :</b> You must not have the DBA privilege, and you must be assigned to the database schema.</p> <p><b>Permissions:</b> Grant the following permissions:</p> <pre>grant create session</pre>
Microsoft SQL Server	<p><b>Required:</b> Set 'read_committed_snapshot' to ON by executing:</p> <ol style="list-style-type: none"> <li>1. <code>alter database &lt;amx-database&gt; set read_committed_snapshot on</code></li> <li>2. Use the case insensitive collation setting for &lt;amx-database&gt;</li> <li>3. Assign &lt;amx-user&gt; the default database &lt;amx-database&gt;</li> </ol> <p><b>Permissions:</b> grant db_datareader, db_datawriter to &lt;amx-user&gt; for the &lt;amx-database&gt;.</p>
IBM DB2	<p><b>Required:</b> Configure the database with a 32KB page size (instead of the default 4KB page size).</p> <p><b>Permissions:</b> Create dmluser with connect database permission.</p>

Database Type	Configuration Notes
PostgreSQL (Starting with TIBCO ActiveMatrix Hotfix 002)	<ol style="list-style-type: none"> <li>1. Create the database user using pgAdmin or SQL Shell and grant required privilege.</li> <li>2. Create the database. The user created in the step a must be the owner of the database.</li> <li>3. In pgAdmin or SQL shell, run the following queries for the database created in the step b : <pre>CREATE FUNCTION pg_catalog.text(bigint) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int8out(\$1));'; CREATE CAST (bigint AS text) WITH FUNCTION pg_catalog.text(bigint) AS IMPLICIT;  CREATE FUNCTION pg_catalog.text(integer) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int4out(\$1));'; CREATE CAST (integer AS text) WITH FUNCTION pg_catalog.text(integer) AS IMPLICIT;  CREATE FUNCTION pg_catalog.text(smallint) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int2out(\$1));'; CREATE CAST (smallint AS text) WITH FUNCTION pg_catalog.text(smallint) AS IMPLICIT;</pre> </li> </ol>

3. Start the database server.



If you use an HSQLDB external database, concurrent user access to the Administrator server is not supported.

### Database Requirements For DDL Generator Users

ActiveMatrix supports a DDL generator utility that you can use before you run TIBCO Configuration Tool. When you use DDL scripts produced by the DDL generator, you need different database permissions than if you do not use DDL scripts. The database user must have connect and resource privileges, and must not have DBA privileges. The database user must be assigned to the default schema.

### Components Configured by the Create TIBCO ActiveMatrix Administrator Server Wizard

The following table summarizes the components that are configured in the Create TIBCO ActiveMatrix Administrator Server wizard, their function, and the decisions you must take, the information you must gather, and actions you must perform before running the wizard.

Component	Function	Options and Actions
<a href="#">Administrator Server</a>	Administers TIBCO ActiveMatrix applications and infrastructure.	Provide the name of the communication group within which status messages are exchanged and the name of the Administrator server. Provide communication properties for the Administrator server.
<a href="#">TIBCO Host Instance</a>	The TIBCO Host instance that manages the SystemNode node on which the Administrator server runs.	Provide configuration details for the TIBCO Host instance.

Component	Function	Options and Actions
Development Node	A node on which to deploy applications.	Provide the name and management port of the development node and the name of the environment that contains the node. If you intend to complete the tutorials in <i>Administration Tutorials</i> , you must create the development node, accept the default values for the environment and node names, and deploy all product applications on the development node. Customize the name and management port of the node and the name of the environment that contains the node.
<a href="#">Notification and Messaging Bus Server</a>	Propagates status messages between hosts, nodes, and the ActiveMatrix Administrator server and messages between applications.	Provide configuration details for the Enterprise Message Service server.
<a href="#">Database</a>	Stores ActiveMatrix Administrator configuration data.	Choose an internal or external database. If you choose an external database, provide configuration details for the database server.
<a href="#">Authentication Realm</a>	Stores user and group data.	<p>Choose a database or LDAP authentication realm. Provide configuration details for the authentication realm.</p> <ul style="list-style-type: none"> <li>• A database authentication realm stores user and group authentication data in a database. Users and groups in this realm can be edited within ActiveMatrix Administrator. You have the option to use the same database for authentication and administration data.</li> </ul> <p>If you choose database, and are using a database different than the one the ActiveMatrix Administrator server uses, provide the configuration details for the database server. See <a href="#">Database Requirements</a>.</p> <ul style="list-style-type: none"> <li>• An LDAP authentication realm uses the user and group authentication data stored in an LDAP server. Users and groups in this realm can only be edited with LDAP server management tools.</li> </ul> <p>If you choose an LDAP realm, the LDAP server must be running.</p>
<a href="#">TIBCO Credential Server</a>	Provides credentials to enable secure interactions between ActiveMatrix Administrator servers, hosts, and nodes.	Choose an autogenerated or external keystore. If you choose an external keystore, provide configuration details for the keystore.

Component	Function	Options and Actions
<a href="#">Logging Notification Server</a>	A log service is a TIBCO ActiveMatrix application that offers logging services.	Choose the ActiveMatrix Administrator notification server or another notification server. If the latter, provide the notification server.
<a href="#">Log Service</a>	Aggregates and stores log entry data.	Choose the ActiveMatrix Administrator database or another database. If you are using a database different than the one the ActiveMatrix Administrator server uses, see <a href="#">Database Requirements</a> .
<a href="#">Payload Service</a>	Stores large payloads associated with log entries.	Choose the ActiveMatrix Administrator database or another database. If you do not use the ActiveMatrix Administrator database, see <a href="#">Database Requirements</a> .

Field	Description
Configure to Secure All Communication with SSL	<p>Check to secure all communication channels with SSL. When you select this checkbox, the Enable SSL checkbox on the Notification and Messaging Bus Server and ActiveMatrix Administrator server screens are selected. See <a href="#">Secure Communication Channels</a> for background information.</p> <p>Default: Cleared.</p>

## Administrator Server Configuration Details

The Administrator Server Configuration Details screen is used to specify the enterprise name and the name of the Administrator Server instance.

Field	Description
Enterprise Name	<p>Communication group for status messages that are sent between the Administrator server, the hosts that are bound to the server, and the nodes that are managed by those hosts.</p> <p>Default:</p> <ul style="list-style-type: none"> <li>amxadmin for ActiveMatrix Administrator</li> </ul> <p>The enterprise name specified here is displayed, by default, on the ActiveMatrix Administrator login banner as the default text, in default colors. The banner text and colors can be customized using the following properties in the <code>SystemNode.tra</code> file:</p> <ul style="list-style-type: none"> <li><code>java.property.com.tibco.admin.gui.login.screen.banner.text=&lt;Login Banner Text&gt;</code> Banner text for the Login screen.</li> <li><code>java.property.com.tibco.admin.gui.login.screen.banner.text.fontColor=&lt;RGB, HEX or HTML Color Name&gt;</code> Banner color for the Login screen.</li> <li><code>java.property.com.tibco.admin.gui.topPanel.banner.text=&lt;Navigation Banner Text&gt;</code> Banner text for the Navigation page.</li> </ul> <p>Both Banner texts, if not configured explicitly with System properties, currently display the name of the TIBCO Enterprise specified in the TIBCO Configuration Tool during Enterprise creation. A maximum of 80 characters of the Banner text are displayed, after which they are truncated and the complete text is displayed via a mouse-over HTML Tooltip.</p>
Server Name	<p>Name of the Administrator server.</p> <p>Default:</p> <ul style="list-style-type: none"> <li>instanceOne for ActiveMatrix Administrator</li> </ul>

## Administrator Server TIBCO Host Configuration


Each Administrator server runs on a TIBCO Host instance. You can specify the instance on which the server will run, configure server characteristics such as a Windows shortcut, and specify the environment and the node.

Field	Description
Machine Name	Name of the machine on which the TIBCO Host instance runs. The value of this property must either be a hostname resolvable through DNS or 0.0.0.0 or IP address.  Default: <i>machineName</i> , where <i>machineName</i> is the machine on which TIBCO Configuration Tool is being executed.
Port	Management port of the TIBCO Host instance.  Default: 6051.
Register as Windows Service	Select to register the TIBCO Host instance as a Windows service named TIBCO ActiveMatrix Admin- <i>enterpriseName-serverName</i> with the startup type Automatic. The service is not started.  Default: Clear.
Create Windows Shortcut	Select to add a shortcut named TIBCO ActiveMatrix Admin- <i>enterpriseName-serverName</i> that points to <i>CONFIG_HOME\tibcohost\Admin-<i>enterpriseName-serverName</i>\host\bin\tibcohost.exe</i> to the Windows desktop.  Default: Clear.
Create Development Node	Select to create a development environment and node . When selected, the Environment Name, Node Name, and Node Management Port fields display. Default: Selected
Environment Name	Name of the environment that contains the node.  Default: <ul style="list-style-type: none"><li>• DevEnvironment for ActiveMatrix</li></ul>
Node Name	Name of the node.  Default: <ul style="list-style-type: none"><li>• DevNode for ActiveMatrix</li></ul>
Node Management Port	Management port of the node.  Default: 6038.



## Administrator Server Connection Settings

The Administrator Server Connection Settings screen is used to specify non-default adapters and ports and to enable and configure SSL for the external HTTP port. You can also choose to enable an HTTP load balancer.

Field	Description
Network Adapter	Address of the network adapter on the machine on which the Administrator server runs. The default is set to 0.0.0.0 so that Administrator will listen on all network adapters (including http://localhost and http://hostname). If you leave the default, clients can connect to the Administrator server using any of the conventions (localhost, IP address, hostname). The value of this property must either be a hostname resolvable through DNS or 0.0.0.0; it cannot be an IP address.
Management Port	Management port of the node that runs Administrator server. Default: Depends on the product you are configuring.
External HTTP Port	Port on which Administrator clients access the Administrator server. Default: 8120.
Browser Idle Session Timeout (m)	Length of time before an inactive Administrator GUI login session times out. Default: 30.
Enable SSL for External HTTP Port	Select to secure communication between Administrator server and clients with SSL. When selected, the Self-Signed Certificate and Imported Certificate radio buttons display. Default: Cleared.
Self-Signed Certificate	Indicates that clients can identify the Administrator server with a self-signed certificate. When selected, it uses the self signed certificate from the samples folder.  Do not use a self-signed certificate in production environments. Default: Selected.
Imported Certificate	Indicates that clients can identify the Administrator server with a certificate imported into the Administrator server. When selected, the Keystore fields and Fetch Keystore button are enabled.
Keystore Location	Location of the keystore to import.
Keystore Type	Type of keystore.
Keystore Password	Password that protects the keystore.
Fetch Keystore	When you click this button, you can select one of the available key aliases, specify the keystore password, and click Verify Keystore to verify that the password you entered is valid.

## Administrator Server Internal HTTP Port



Field	Description
Internal HTTP Port	Number of the internal Administrator HTTP port. Default: 19767.
Enable SSL	Select to secure communication between Administrator server and hosts with SSL. Default: Cleared.

## Administrator Server Notification and Messaging Bus Server

The notification server is an Enterprise Message Service server that delivers status messages sent by hosts and nodes to the Administrator server.

As part of configuration, set up the notification and messaging bus server. To use SSL, see [Secure Communication Channels](#). To enable SSL communications, see [SSL Requirements](#).

Field	Description
Machine Name Port List	Comma-separated list of <i>machinename:port</i> addresses for a TIBCO Enterprise Message Service (EMS) server.  Default: <i>machinename:port</i> , where <i>machinename</i> is the host on which TIBCO Configuration Tool is being executed and <i>port</i> is 7222. The default <i>machinename:port</i> is <code>tcp://hostname:7222</code> . If the Enterprise Message Service server is SSL enabled, the hostname is <code>ssl://hostname:7222</code> .
Username	Username for the EMS server. The user must have administrator privileges in the EMS server. If the user does not have administrator privileges, configure your EMS server as described in <a href="#">Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users</a> . Default: admin.
Password	Password for the EMS user. Default: None.
TIBCO Enterprise Message Service server is SSL enabled. Specify a trust store to establish trust with this server.	Select to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled. Default: Cleared.

Field	Description
No Messaging Bus	<p>See <a href="#">Determining Whether an Enterprise Needs a Messaging Bus</a>.</p> <p>Select to create an enterprise that does not use a messaging bus. This is useful in scenarios where you do not want to distribute entities (components and bindings) of an application to different Nodes and hence do not need a messaging bus. In such scenarios, applications can be deployed even if the messaging bus is down or not available.</p> <ul style="list-style-type: none"> <li>If <b>No Messaging Bus</b> is selected, it creates an enterprise that does not use a messaging bus.</li> </ul> <div>  <p>Do not use select this checkbox if you are setting up TIBCO ActiveMatrix BPM. It could result in the failure of the TIBCO ActiveMatrix BPM setup.</p> </div> <ul style="list-style-type: none"> <li>If <b>No Messaging Bus</b> is cleared, it creates an enterprise that uses a messaging bus. You can then choose to create an environment with or without a messaging bus.</li> </ul> <div>  <p>Even if <b>No Messaging Bus</b> is cleared and you create an enterprise that uses the messaging bus, you can later configure the enterprise to stop using a messaging bus. For more information, see section "Configuring an Enterprise to Stop Using a Messaging Bus" of <i>TIBCO ActiveMatrix Service Grid Administration Guide</i>.</p> </div> <p>Default: Cleared.</p> <p>For more information on how to configure messaging bus settings related to an environment, see <i>TIBCO ActiveMatrix Service Grid Administration Guide</i>.</p>
Test Connection	Click the <b>Test Connection</b> button to test connection to TIBCO Enterprise Message Service (EMS) server.



This is an example of a scenario when the TIBCO Enterprise Message Service server is SSL enabled. In this example, Enterprise Message Service server is configured with SSL for GenericConnectionFactory. Edit the `factories.conf` and include the following:

```
[GenericConnectionFactory]
type = generic
url = ssl://7243
ssl_verify_host = enabled
ssl_trusted = EMS_HOME/version/samples/certs/server_root_cert.pem
```

In the `tibemsd.conf`, include the following:

```
listen = ssl://7243
authorization = enabled
ssl_server_identity = EMS_HOME/version/samples/certs/server.cert.pem
ssl_server_key = EMS_HOME/version/samples/certs/server.key.pem
ssl_password = password
ssl_server_trusted = EMS_HOME/version/samples/certs/server_root.cert.pem
```

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	<p>Type of the keystore: JKS or JCEKS.</p> <p>Default: JKS.</p>
Keystore Password	Password that protects the keystore.

### Administrator Server Enterprise Message Service Connection Factory

This screen helps you select a connection factory configured for fault-tolerance. This must match with your input of multiple Enterprise Message Service servers.

Field	Description
Connection Factory Name	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• GenericConnectionFactory</li> <li>• QueueConnectionFactory</li> <li>• TopicConnectionFactory</li> <li>• FTTopicConnectionFactory</li> <li>• SSL TopicConnectionFactory</li> <li>• SSL QueueConnnectionFactory</li> <li>• FTQueueConnectionFactory</li> </ul>

### Administrator Server Database Details

You can choose to use the Administrator server with a default in-process database during development. In production systems, use an external database instead. This screen allows you to configure database details.

Field	Description
Use Default In-Process Database	<p>Select to use the embedded in-memory database, or clear to use an external database. If cleared, the database configuration fields display.</p> <p>Default: Selected.</p>

If you decide to use a non-default database, the wizard prompts you for database details.





Use the default embedded database only during development.

If you are using an external database, see [Database Requirements](#). To enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).



The properties that the wizard sets in the `build.properties` file depend on the context in which the prompts are displayed. By default, specify the properties for the Administrator Server database and the information is then used for the Notification Service database, the Log Service database, and the Payload Service database. You can, however, overwrite the values for the Notification Service, Log Service, and Payload Service, and you can change them in the `build.properties` file.

Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (<code>postgresql-42.2.8.jar</code> is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (<code>postgresql-42.2.8.jar</code> is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>
Database URL	<p>URL of the external database.</p> <p>Default: <code>jdbc:hsqldb:hsql://localhost:1234/amx.</code></p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the <code>pg_hba.conf</code> file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the <code>pg_hba.conf</code> file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: <code>sa</code>.</p>

Field	Description
Password	External database password. Default: None.
Max Connections	Maximum number of database connections to allocate. Default: 10.
Database Server is SSL Enabled	Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled. Default: Cleared.   PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002.
Test Connection	Click the <b>Test Connection</b> button to ensure that you can connect to the database.

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.  <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS. Default: JKS.
Keystore Password	Password that protects the keystore.

### Administrator Server Authentication Realm

Administrator stores information about users and groups in an authentication realm. You can let Administrator store the information in a database or in LDAP. TIBCO Configuration Tool will then prompt you for more information about the authentication realm.

Field	Description
<b>Authentication Realm</b>	

Field	Description
Realm Type	Type of authentication realm: <ul style="list-style-type: none"> <li>Database - See <a href="#">Administrator Server Database Authentication Realm</a></li> <li>LDAP - See <a href="#">Administrator Server LDAP Authentication Realm</a></li> </ul> Default: Database.
<b>Superuser Credentials</b>	
Username	Name of the initial superuser. Default: root.
Password	Password of the superuser. Default: t. In the properties file, this value is obfuscated.

### Administrator Server Database Authentication Realm

If you select a database authentication realm, Administrator stores information about users and groups in a database. You can select the same database as the Administrator server, or configure a different database.

Field	Description
Use ActiveMatrix Administrator Server Database	Select if the database authentication realm should use the same database as the Administrator server. If cleared, the database configuration fields display. Default: Selected.

If you decide to use a non-default database, the wizard prompts you for database details.




Use the default embedded database only during development.


If you are using an external database, see [Database Requirements](#). To enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).



The properties that the wizard sets in the `build.properties` file depend on the context in which the prompts are displayed. By default, specify the properties for the Administrator Server database and the information is then used for the Notification Service database, the Log Service database, and the Payload Service database. You can, however, overwrite the values for the Notification Service, Log Service, and Payload Service, and you can change them in the `build.properties` file.

Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (postgresql-42.2.8.jar is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (postgresql-42.2.8.jar is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>
Database URL	<p>URL of the external database.</p> <p>Default: jdbc:hsqldb:hsq1://localhost:1234/amx.</p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the pg_hba.conf file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the pg_hba.conf file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: sa.</p>
Password	<p>External database password.</p> <p>Default: None.</p>
Max Connections	<p>Maximum number of database connections to allocate.</p> <p>Default: 10.</p>



Field	Description
Database Server is SSL Enabled	<p>Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.</p> <p>Default: Cleared.</p> <div>  <div> <p>PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002.</p> </div> </div>
Test Connection	Click the <b>Test Connection</b> button to ensure that you can connect to the database.

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	<p>Type of the keystore: JKS or JCEKS.</p> <p>Default: JKS.</p>
Keystore Password	Password that protects the keystore.

### Administrator Server LDAP Authentication Realm

If you select an LDAP authentication realm, Administrator stores information about users and groups in LDAP. You are prompted for the user and password, name resolution context, and server URLs. You can also specify the user search configuration and optional group information.

If you intend to enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).

Field	Description
Bind DN Name	<p>Distinguished name or name of the superuser to be used to connect to the server.</p> <p>Default: uid=Manager,ou=people,dc=example,dc=com.</p>
Password	<p>LDAP server password.</p> <p>Default: None.</p>

Field	Description
Context Factory	Factory object that provides the starting point for resolution of names within the LDAP server.  Default: com.sun.jndi.ldap.LdapCtxFactory
Machine Name Port List	Comma-separated list of URLs for an LDAP server. To achieve fault tolerance, you can specify multiple URLs. For example, server1.example.com:686, server2.example.com:1686.  Default: <i>machinename</i> :389, where <i>machinename</i> is the machine on which TIBCO Configuration Tool is being executed.
Fetch DN	You can retrieve the base DN (distinguished name) of the LDAP server.
<b>User Search Configuration</b>	
User Search Base DN (optional)	Base distinguished name from which the search starts.  Default: ou=people,ou=na,dc=example,dc=org
User Search Expression (optional)	Expression used for searching a user. For example: (CN=%U). '%U' is replaced by the username being searched for. You can define any complex filter such as (&cn=%U)(objectClass=account)).  Default: (&(uid={0})(objectclass=person)).
User Attribute with User Name (optional)	Name of the attribute in the user object that contains the user's name.  Default: uid.
Search Timeout (ms)	Time to wait for a response from the LDAP server. A values less than 90 seconds yields in a warning message.  Default: 30000.
Follow Referrals	Select to follow LDAP referrals. If you select this check box, requests to LDAP can be redirected to another server. Use this check box to indicate that the LDAP information might be available at another location, or possibly at another server or servers.  Ask your LDAP administrator whether LDAP referrals are used in your domain.

Field	Description
Group Indication (optional)	Specifies how a user's group memberships are found. Administrator uses group information when a user, once authenticated, performs other activities in the system. Options: <ul style="list-style-type: none"> <li><b>Group has users</b> - List of users that belong to the group. When selected, the Group Attribute with User Names field is enabled.</li> <li><b>User has groups</b> - List of groups to which the user belongs. When selected, the User Attribute with Group Names field is enabled.</li> </ul> Default: Group has users.

Field	Description
Group Search Base DN (optional)	Base distinguished name from which the search for the group starts. Default: ou=groups,ou=na,dc=example,dc=org.
Group Search Expression (optional)	Search by matching this expression against potential groups. Default: (&(cn={0})(objectClass=groupofuniqueNames)).
Group Attribute with User Names (optional)	Name of the attribute in the group object containing its users. Example: uniqueMember (OpenLDAP) or member (ActiveDirectory). Default: uniqueMember.
Group Attribute with Group Name (optional)	Name of the attribute in the group object that contains the name of the group. Example: cn (OpenLDAP) or sAMAccountName (ActiveDirectory). Default: cn.
Group Attribute Subgroup Names (optional)	Name of the attribute in the group object that contains its subgroups. Example: uniqueMember (OpenLDAP) or member (ActiveDirectory). Default: uniqueMember.
User Attribute with Group Names	Name of the attribute in the user object that lists the groups to which the user belongs. Default: None.
Group Search Scope Subtree	When searching the group, indicate whether to traverse into the subtree or to search only under the group base distinguished name. Default: Selected.

Field	Description
<b>LDAP Realm</b>	
User Search Scope Subtree	Select to have the search include the entire subtree starting at the base DN. Otherwise, search only the nodes one level below the base DN. Default: Selected.
Security Authentication	Value of Simple Authentication and Security Layer (SASL) authentication protocol to use. Values are implementation-dependent. Some possible values are simple, none, strong. Default: simple.
<b>LDAP Authentication</b>	
LDAP Server is SSL Enabled	Select to enable the LDAP server for SSL. When selected, the SSL Keystore Configuration fields are enabled. Default: Cleared.

Field	Description
Test Connection	Click the <b>Test Connection</b> button to ensure that you can connect to the LDAP database.

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	<p>Type of the keystore: JKS or JCEKS.</p> <p>Default: JKS.</p>
Keystore Password	Password that protects the keystore.

### Administrator Server TIBCO Credential Server Details

You can specify credential server details to identify the TIBCO Credential Server that you want to use with your Administrator server installation.

Field	Description
Network Adapter	<p>Address of the network adapter on the machine on which TIBCO Credential Server runs. The default is set to 0.0.0.0 so that TIBCO Credential Server will listen on all network adapters (including http://localhost and http://hostname). With the default setting, clients can connect to TIBCO Credential Server using any of the conventions (localhost, IP address, hostname). The value of this property must either be a hostname resolvable through DNS or 0.0.0.0; it cannot be an IP address.</p> <p>Default: 0.0.0.0.</p>
Port	<p>Management port number of the node, SystemNode, that runs TIBCO Credential Server.</p> <p>Default: 6041.</p>
Username	<p>User identifier for TIBCO Credential Server clients.</p> <p>Default: user1.</p>
Password	Password for the client.

## Administrator Server TIBCO Credential Server Keystore

If you enable SSL, you can use Administrator server with an auto-generated keystore or specify keystore information.

Field	Description
Auto-generated Keystore	Select to generate a TIBCO Credential Server keystore will be generated. When selected, the Common Name field displays. Default: Selected.
Common Name	Issuer name of TIBCO Credential Server. Default: amxadmin.
Provided Keystore	Check to provide TIBCO Credential Server keystore information. When selected, the keystore fields display. Default: Cleared.
Keystore Location	Location of the keystore.
Keystore Type	Type of keystore. Default: Autodetect.
Keystore Password	Password for the keystore.
Fetch Keystore	When you click this button, you can select one of the available key aliases, specify the keystore password, and click <b>Verify Keystore</b> to verify that the password you entered is valid.
Key Alias	Name of the alias used to access the identity
Key Password	Password for the alias

## Administrator Server Logging Notification Server

A log service is a TIBCO ActiveMatrix application that offers logging services. The log service application `com.tibco.amx.commonlogging.logservice.app` is deployed in the environment `SystemEnvironment` on `SystemNode`, the node that runs the Administrator server.

Field	Description
Use ActiveMatrix Administrator Notification and Messaging Bus Server	Select if you want the logging service to use the same notification server as the Administrator server. If cleared, the wizard allows you to configure the logging service explicitly. Default: Selected.

As part of configuration, set up the notification and messaging bus server. To use SSL, see [Secure Communication Channels](#). To enable SSL communications, see [SSL Requirements](#).

Field	Description
Machine Name Port List	<p>Comma-separated list of <i>machinename:port</i> addresses for a TIBCO Enterprise Message Service (EMS) server.</p> <p>Default: <i>machinename:port</i>, where <i>machinename</i> is the host on which TIBCO Configuration Tool is being executed and <i>port</i> is 7222. The default <i>machinename:port</i> is <code>tcp://hostname:7222</code>. If the Enterprise Message Service server is SSL enabled, the hostname is <code>ssl://hostname:7222</code>.</p>
Username	<p>Username for the EMS server. The user must have administrator privileges in the EMS server. If the user does not have administrator privileges, configure your EMS server as described in <a href="#">Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users</a>.</p> <p>Default: admin.</p>
Password	<p>Password for the EMS user.</p> <p>Default: None.</p>
TIBCO Enterprise Message Service server is SSL enabled. Specify a trust store to establish trust with this server.	<p>Select to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.</p> <p>Default: Cleared.</p>
Test Connection	Click the <b>Test Connection</b> button to test connection to TIBCO Enterprise Message Service (EMS) server.



This is an example of a scenario when the TIBCO Enterprise Message Service server is SSL enabled. In this example, Enterprise Message Service server is configured with SSL for GenericConnectionFactory. Edit the `factories.conf` and include the following:

```
[GenericConnectionFactory]
type = generic
url = ssl://7243
ssl_verify_host = enabled
ssl_trusted = EMS_HOME/version/samples/certs/server_root_cert.pem
```

In the `tibemsd.conf`, include the following:

```
listen = ssl://7243
authorization = enabled
ssl_server_identity = EMS_HOME/version/samples/certs/server.cert.pem
ssl_server_key = EMS_HOME/version/samples/certs/server.key.pem
ssl_password = password
ssl_server_trusted = EMS_HOME/version/samples/certs/server_root.cert.pem
```

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>

Field	Description
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS. Default: JKS.
Keystore Password	Password that protects the keystore.

### Administrator Server Log Service Database

A log service is a TIBCO ActiveMatrix application that offers logging services. The log service application is deployed in the environment `SystemEnvironment` on `SystemNode`, the node that runs the Administrator server. A log service receives log entries sent to a JMS destination and stores the entries in a database.

If you did not deploy the logging and payload services when you created the Administrator server using the TIBCO Configuration Tool, see `TIBCO_HOME\administrator\version\scripts\logging\readme.txt`.

Field	Description
Use ActiveMatrix Administrator Server Database	Select to have the log service use the same database as the Administrator server. If cleared, the database fields display. Default: Selected.

If you decide to use a non-default database, the wizard prompts you for database details.




Use the default embedded database only during development.


If you are using an external database, see [Database Requirements](#). To enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).



The properties that the wizard sets in the `build.properties` file depend on the context in which the prompts are displayed. By default, specify the properties for the Administrator Server database and the information is then used for the Notification Service database, the Log Service database, and the Payload Service database. You can, however, overwrite the values for the Notification Service, Log Service, and Payload Service, and you can change them in the `build.properties` file.

Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (postgresql-42.2.8.jar is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (postgresql-42.2.8.jar is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>
Database URL	<p>URL of the external database.</p> <p>Default: jdbc:hsqldb:hsq1://localhost:1234/amx.</p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the pg_hba.conf file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the pg_hba.conf file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: sa.</p>
Password	<p>External database password.</p> <p>Default: None.</p>
Max Connections	<p>Maximum number of database connections to allocate.</p> <p>Default: 10.</p>



Field	Description
Database Server is SSL Enabled	<p>Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.</p> <p>Default: Cleared.</p> <div>  <div> <p>PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002.</p> </div> </div>
Test Connection	Click the <b>Test Connection</b> button to ensure that you can connect to the database.

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	<p>Type of the keystore: JKS or JCEKS.</p> <p>Default: JKS.</p>
Keystore Password	Password that protects the keystore.

### Administrator Server Payload Service Database

A payload service supports archiving, persisting and retrieving large size payload data. It is an independent service and does not depend on a log service. However, a log record sent to a log service can include a payload URL field to link a log message and payload data. You can store payload data in the same database used by Administrator server or use another database.

If you did not deploy the logging and payload services when you created the Administrator server using the TIBCO Configuration Tool, see *TIBCO\_HOME\administrator\version\scripts\logging\readme.txt*.

Field	Description
Use ActiveMatrix Administrator Server Database	<p>Select to have the payload service use the same database as the Administrator server. If cleared, the database configuration fields display to let you specify database information.</p> <p>Default: Selected.</p>

If you decide to use a non-default database, the wizard prompts you for database details.





Use the default embedded database only during development.

If you are using an external database, see [Database Requirements](#). To enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).



The properties that the wizard sets in the `build.properties` file depend on the context in which the prompts are displayed. By default, specify the properties for the Administrator Server database and the information is then used for the Notification Service database, the Log Service database, and the Payload Service database. You can, however, overwrite the values for the Notification Service, Log Service, and Payload Service, and you can change them in the `build.properties` file.

Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (<code>postgresql-42.2.8.jar</code> is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (<code>postgresql-42.2.8.jar</code> is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>
Database URL	<p>URL of the external database.</p> <p>Default: <code>jdbc:hsqldb:hsql://localhost:1234/amx.</code></p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the <code>pg_hba.conf</code> file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the <code>pg_hba.conf</code> file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: <code>sa.</code></p>

Field	Description
Password	External database password. Default: None.
Max Connections	Maximum number of database connections to allocate. Default: 10.
Database Server is SSL Enabled	Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled. Default: Cleared.   PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002.
Test Connection	Click the <b>Test Connection</b> button to ensure that you can connect to the database.

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.  <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS. Default: JKS.
Keystore Password	Password that protects the keystore.

## Summary

With each TIBCO Configuration Tool wizard's summary screen, you can check the configuration that you specified and see the effects of that configuration. You can click **Back** to make changes, save the configuration for use by the silent installer, or click **Configure** to start the configuration. If you are using the console configuration tool, you can perform the same actions by typing single-letter commands, as prompted.

Field	Description
Session Scripts and Log Folder	Folder containing the script configured in the wizard and the log file if the script is executed.

Field	Description
Administrator URL	If an Administrator server was configured in the wizard, a link to the URL of the Administrator server.
Actions	Actions that will be performed when you click the <b>Configure</b> button. Select the check boxes next to the actions you want to execute.
Products to Deploy	Product applications that will be deployed on the node if one has been configured. All products are selected by default. Clear the check boxes next to products you do not want deployed.  If you do not deploy the logging and payload services when you created the Administrator server using the TIBCO Configuration Tool, see <code>TIBCO_HOME\administrator\version\scripts\logging\readme.txt</code> .
Save	Saves the configuration in the location specified in the Session Scripts and Log Folder field.
Configure	Saves the configuration in the location specified in the Session Scripts and Log Folder field and performs the actions specified in Actions and Products to Deploy.
Cancel	Returns to the wizard selector screen.

## Create TIBCO ActiveMatrix Policy Director Governance Administrator Server

The Create TIBCO ActiveMatrix Policy Director Governance Administrator Server wizard guides you through the process of creating a TIBCO ActiveMatrix Policy Director Governance Administrator Server. Many of the configuration screens prompt for the same information as the Administrator server wizard, but a few new screens prompt for TIBCO ActiveMatrix Policy Director Governance information.

The Create TIBCO ActiveMatrix Policy Director Governance Administrator Server wizard allows you to configure many aspects of your server including the database, authentication method, log service, and more. You can review this wizard documentation before you start configuration to decide how you want to set up the server.



The wizard takes 15 minutes or more to complete depending on the configuration options.

### Database Requirements

When you run the wizard, you specify a database for Administrator server and for several system services. If you are using an external database (and do not use HSQLDB as an external database), set up the external database before you run the wizard.

1. Package, install, and configure the database driver using the [Configure Third-Party Driver](#) wizard.
2. Configure the external database.

Database	Configuration Notes
<b>Oracle 12c PDB</b>	<p>The database user must have to be set up as follows:</p> <ul style="list-style-type: none"> <li>• Must have connect and resource privileges</li> <li>• Must be assigned to the default schema</li> <li>• Cannot have dba privileges</li> </ul> <p>Run the command:</p> <pre>alter pluggable database ORCLPDB open; alter session set container =ORCLPDB; create user amxuser identified by password; grant create session,connect, resource, create table, create session, unlimited tablespace to amuser;</pre>
<b>Microsoft SQL Server</b>	<ul style="list-style-type: none"> <li>• Run the command <pre>alter database DB Name set read_committed_snapshot on.</pre> </li> <li>• Make sure that the database user is assigned the default database and has the db_owner role.</li> <li>• Use the case insensitive collation setting.</li> </ul>
<b>IBM DB2</b>	<p>Configure the database with a 32KB page size (instead of the default 4KB page size).</p>
<b>PostgreSQL (Starting with TIBCO ActiveMatrix Hotfix 002)</b>	<ol style="list-style-type: none"> <li>1. Create the database user using pgAdmin or SQL Shell and grant required privilege.</li> <li>2. Create the database. The user created in the step a must be the owner of the database.</li> <li>3. In pgAdmin or SQL shell, run the following queries for the database created in the step b : <pre>CREATE FUNCTION pg_catalog.text(bigint) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int8out(\$1));'; CREATE CAST (bigint AS text) WITH FUNCTION pg_catalog.text(bigint) AS IMPLICIT;  CREATE FUNCTION pg_catalog.text(integer) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int4out(\$1));'; CREATE CAST (integer AS text) WITH FUNCTION pg_catalog.text(integer) AS IMPLICIT;  CREATE FUNCTION pg_catalog.text(smallint) RETURNS text STRICT IMMUTABLE LANGUAGE SQL AS 'SELECT textin(int2out(\$1));'; CREATE CAST (smallint AS text) WITH FUNCTION pg_catalog.text(smallint) AS IMPLICIT;</pre> </li> </ol>

3. Start the database server.



If you use an HSQLDB external database, concurrent user access to Administrator server is not supported.

### TIBCO ActiveMatrix Policy Director Governance Administrator Server Selection

You can choose an existing Administrator Server or create a new Administrator Server to manage TIBCO ActiveMatrix Policy Director Governance services.

Field	Description
<b>Select a TIBCO ActiveMatrix Administrator Server Configuration</b>	
Select a TIBCO ActiveMatrix Administrator Server Configuration	Select to use an existing Administrator server for TIBCO ActiveMatrix Policy Director Governance. If you select this option, configuration data of the existing server are used, but you are prompted for some information that is specific to TIBCO ActiveMatrix Policy Director Governance. Default: Unchecked
TIBCO Configuration folder	Directory for configuration data. Default: C:/ProgramData/environment_name/data
Configuration	Select the Administrator server configuration you want to use.
<b>Create a TIBCO ActiveMatrix Policy Director Governance Administrator Server</b>	
Create a TIBCO ActiveMatrix Policy Director Governance Administrator Server	Check to create a new Administrator server for TIBCO ActiveMatrix Policy Director Governance. If you select this option, the following screens prompt for information about the new server you are creating. Default: Checked

## Administrator Server Configuration Details

The Administrator Server Configuration Details screen is used to specify the enterprise name and the name of the Administrator Server instance.

Field	Description
Enterprise Name	<p>Communication group for status messages that are sent between the Administrator server, the hosts that are bound to the server, and the nodes that are managed by those hosts.</p> <p>Default:</p> <ul style="list-style-type: none"> <li>amxadmin for ActiveMatrix Administrator</li> </ul> <p>The enterprise name specified here is displayed, by default, on the ActiveMatrix Administrator login banner as the default text, in default colors. The banner text and colors can be customized using the following properties in the <code>SystemNode.tra</code> file:</p> <ul style="list-style-type: none"> <li><code>java.property.com.tibco.admin.gui.login.screen.banner.text=&lt;Login Banner Text&gt;</code> Banner text for the Login screen.</li> <li><code>java.property.com.tibco.admin.gui.login.screen.banner.text.fontColor=&lt;RGB, HEX or HTML Color Name&gt;</code> Banner color for the Login screen.</li> <li><code>java.property.com.tibco.admin.gui.topPanel.banner.text=&lt;Navigation Banner Text&gt;</code> Banner text for the Navigation page.</li> </ul> <p>Both Banner texts, if not configured explicitly with System properties, currently display the name of the TIBCO Enterprise specified in the TIBCO Configuration Tool during Enterprise creation. A maximum of 80 characters of the Banner text are displayed, after which they are truncated and the complete text is displayed via a mouse-over HTML Tooltip.</p>
Server Name	<p>Name of the Administrator server.</p> <p>Default:</p> <ul style="list-style-type: none"> <li>instanceOne for ActiveMatrix Administrator</li> </ul>

## Administrator Server TIBCO Host Configuration


Each Administrator server runs on a TIBCO Host instance. You can specify the instance on which the server will run, configure server characteristics such as a Windows shortcut, and specify the environment and the node.

Field	Description
Machine Name	Name of the machine on which the TIBCO Host instance runs. The value of this property must either be a hostname resolvable through DNS or 0.0.0.0 or IP address.  Default: <i>machineName</i> , where <i>machineName</i> is the machine on which TIBCO Configuration Tool is being executed.
Port	Management port of the TIBCO Host instance.  Default: 6051.
Register as Windows Service	Select to register the TIBCO Host instance as a Windows service named TIBCO ActiveMatrix Admin- <i>enterpriseName-serverName</i> with the startup type Automatic. The service is not started.  Default: Clear.
Create Windows Shortcut	Select to add a shortcut named TIBCO ActiveMatrix Admin- <i>enterpriseName-serverName</i> that points to <i>CONFIG_HOME\tibcohost\Admin-<i>enterpriseName-serverName</i>\host\bin\tibcohost.exe</i> to the Windows desktop.  Default: Clear.
Create Development Node	Select to create a development environment and node . When selected, the Environment Name, Node Name, and Node Management Port fields display. Default: Selected
Environment Name	Name of the environment that contains the node.  Default: <ul style="list-style-type: none"><li>• DevEnvironment for ActiveMatrix</li></ul>
Node Name	Name of the node.  Default: <ul style="list-style-type: none"><li>• DevNode for ActiveMatrix</li></ul>
Node Management Port	Management port of the node.  Default: 6038.




## Administrator Server Connection Settings

The Administrator Server Connection Settings screen is used to specify non-default adapters and ports and to enable and configure SSL for the external HTTP port. You can also choose to enable an HTTP load balancer.

Field	Description
Network Adapter	Address of the network adapter on the machine on which the Administrator server runs. The default is set to 0.0.0.0 so that Administrator will listen on all network adapters (including http://localhost and http://hostname). If you leave the default, clients can connect to the Administrator server using any of the conventions (localhost, IP address, hostname). The value of this property must either be a hostname resolvable through DNS or 0.0.0.0; it cannot be an IP address.
Management Port	Management port of the node that runs Administrator server. Default: Depends on the product you are configuring.
External HTTP Port	Port on which Administrator clients access the Administrator server. Default: 8120.
Browser Idle Session Timeout (m)	Length of time before an inactive Administrator GUI login session times out. Default: 30.
Enable SSL for External HTTP Port	Select to secure communication between Administrator server and clients with SSL. When selected, the Self-Signed Certificate and Imported Certificate radio buttons display. Default: Cleared.
Self-Signed Certificate	Indicates that clients can identify the Administrator server with a self-signed certificate. When selected, it uses the self signed certificate from the samples folder.  Do not use a self-signed certificate in production environments. Default: Selected.
Imported Certificate	Indicates that clients can identify the Administrator server with a certificate imported into the Administrator server. When selected, the Keystore fields and Fetch Keystore button are enabled.
Keystore Location	Location of the keystore to import.
Keystore Type	Type of keystore.
Keystore Password	Password that protects the keystore.
Fetch Keystore	When you click this button, you can select one of the available key aliases, specify the keystore password, and click Verify Keystore to verify that the password you entered is valid.

## Administrator Server Connection Details

The Administrator Server Connection Details screen is used to specify non-default adapters and ports and to enable and configure SSL for the external HTTP port. You can also choose to enable an HTTP load balancer.

Field	Description
Machine Name	Name of the machine on which the Administrator server runs. The default is set to 0.0.0.0 so that Administrator listens on all network adapters (including http://localhost and http://hostname). If you leave the default, clients can connect to the Administrator server using any of the conventions (localhost, IP address, hostname). The value of this property must either be a hostname resolvable through DNS or 0.0.0.0.
Port	Management port of the node that runs Administrator server. Default: Depends on the product you are configuring.
User name	User name for the server.
Password	Password for the user.
Enable SSL for External HTTP Port	Select to secure communication between Administrator server and clients with SSL. When selected, the Self-Signed Certificate and Imported Certificate radio buttons display. Default: Cleared.
Self-Signed Certificate	Indicates that clients can identify the Administrator server with a self-signed certificate. When selected, it uses the self signed certificate from the samples folder.  Do not use a self-signed certificate in production environments. Default: Selected.
Imported Certificate	Indicates that clients can identify the Administrator server with a certificate imported into the Administrator server. When selected, the Keystore fields and Fetch Keystore button are enabled.
Keystore Location	Location of the keystore to import.
Keystore Type	Type of keystore.
Keystore Password	Password that protects the keystore.
Fetch Keystore	When you click this button, you can select one of the available key aliases, specify the keystore password, and click Verify Keystore to verify that the password you entered is valid.

## Administrator Server Internal HTTP Port



Field	Description
Internal HTTP Port	Number of the internal Administrator HTTP port. Default: 19767.
Enable SSL	Select to secure communication between Administrator server and hosts with SSL. Default: Cleared.

## Administrator Server Notification and Messaging Bus Server

The notification server is an Enterprise Message Service server that delivers status messages sent by hosts and nodes to the Administrator server.

As part of configuration, set up the notification and messaging bus server. To use SSL, see [Secure Communication Channels](#). To enable SSL communications, see [SSL Requirements](#).

Field	Description
Machine Name Port List	Comma-separated list of <i>machinename:port</i> addresses for a TIBCO Enterprise Message Service (EMS) server.  Default: <i>machinename:port</i> , where <i>machinename</i> is the host on which TIBCO Configuration Tool is being executed and <i>port</i> is 7222. The default <i>machinename:port</i> is <code>tcp://hostname:7222</code> . If the Enterprise Message Service server is SSL enabled, the hostname is <code>ssl://hostname:7222</code> .
Username	Username for the EMS server. The user must have administrator privileges in the EMS server. If the user does not have administrator privileges, configure your EMS server as described in <a href="#">Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users</a> . Default: admin.
Password	Password for the EMS user. Default: None.
TIBCO Enterprise Message Service server is SSL enabled. Specify a trust store to establish trust with this server.	Select to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled. Default: Cleared.

Field	Description
No Messaging Bus	<p>See <a href="#">Determining Whether an Enterprise Needs a Messaging Bus</a>.</p> <p>Select to create an enterprise that does not use a messaging bus. This is useful in scenarios where you do not want to distribute entities (components and bindings) of an application to different Nodes and hence do not need a messaging bus. In such scenarios, applications can be deployed even if the messaging bus is down or not available.</p> <ul style="list-style-type: none"> <li>If <b>No Messaging Bus</b> is selected, it creates an enterprise that does not use a messaging bus.</li> </ul> <div>  <p>Do not use select this checkbox if you are setting up TIBCO ActiveMatrix BPM. It could result in the failure of the TIBCO ActiveMatrix BPM setup.</p> </div> <ul style="list-style-type: none"> <li>If <b>No Messaging Bus</b> is cleared, it creates an enterprise that uses a messaging bus. You can then choose to create an environment with or without a messaging bus.</li> </ul> <div>  <p>Even if <b>No Messaging Bus</b> is cleared and you create an enterprise that uses the messaging bus, you can later configure the enterprise to stop using a messaging bus. For more information, see section "Configuring an Enterprise to Stop Using a Messaging Bus" of <i>TIBCO ActiveMatrix Service Grid Administration Guide</i>.</p> </div> <p>Default: Cleared.</p> <p>For more information on how to configure messaging bus settings related to an environment, see <i>TIBCO ActiveMatrix Service Grid Administration Guide</i>.</p>
Test Connection	Click the <b>Test Connection</b> button to test connection to TIBCO Enterprise Message Service (EMS) server.



This is an example of a scenario when the TIBCO Enterprise Message Service server is SSL enabled. In this example, Enterprise Message Service server is configured with SSL for GenericConnectionFactory. Edit the `factories.conf` and include the following:

```
[GenericConnectionFactory]
type = generic
url = ssl://7243
ssl_verify_host = enabled
ssl_trusted = EMS_HOME/version/samples/certs/server_root_cert.pem
```

In the `tibemsd.conf`, include the following:

```
listen = ssl://7243
authorization = enabled
ssl_server_identity = EMS_HOME/version/samples/certs/server.cert.pem
ssl_server_key = EMS_HOME/version/samples/certs/server.key.pem
ssl_password = password
ssl_server_trusted = EMS_HOME/version/samples/certs/server_root.cert.pem
```

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	<p>Type of the keystore: JKS or JCEKS.</p> <p>Default: JKS.</p>
Keystore Password	Password that protects the keystore.

### Administrator Server Enterprise Message Service Connection Factory

This screen helps you select a connection factory configured for fault-tolerance. This must match with your input of multiple Enterprise Message Service servers.

Field	Description
Connection Factory Name	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• GenericConnectionFactory</li> <li>• QueueConnectionFactory</li> <li>• TopicConnectionFactory</li> <li>• FTTopicConnectionFactory</li> <li>• SSL TopicConnectionFactory</li> <li>• SSL QueueConnnectionFactory</li> <li>• FTQueueConnectionFactory</li> </ul>

### Administrator Server Database Details

You can choose to use the Administrator server with a default in-process database during development. In production systems, use an external database instead. This screen allows you to configure database details.

Field	Description
Use Default In-Process Database	<p>Select to use the embedded in-memory database, or clear to use an external database. If cleared, the database configuration fields display.</p> <p>Default: Selected.</p>

If you decide to use a non-default database, the wizard prompts you for database details.





Use the default embedded database only during development.

If you are using an external database, see [Database Requirements](#). To enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).



The properties that the wizard sets in the `build.properties` file depend on the context in which the prompts are displayed. By default, specify the properties for the Administrator Server database and the information is then used for the Notification Service database, the Log Service database, and the Payload Service database. You can, however, overwrite the values for the Notification Service, Log Service, and Payload Service, and you can change them in the `build.properties` file.

Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (<code>postgresql-42.2.8.jar</code> is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (<code>postgresql-42.2.8.jar</code> is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>
Database URL	<p>URL of the external database.</p> <p>Default: <code>jdbc:hsqldb:hsql://localhost:1234/amx.</code></p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the <code>pg_hba.conf</code> file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the <code>pg_hba.conf</code> file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: <code>sa</code>.</p>

Field	Description
Password	External database password. Default: None.
Max Connections	Maximum number of database connections to allocate. Default: 10.
Database Server is SSL Enabled	Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled. Default: Cleared.   PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002.
Test Connection	Click the <b>Test Connection</b> button to ensure that you can connect to the database.

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.  <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS. Default: JKS.
Keystore Password	Password that protects the keystore.

### Administrator Server Authentication Realm

Administrator stores information about users and groups in an authentication realm. You can let Administrator store the information in a database or in LDAP. TIBCO Configuration Tool will then prompt you for more information about the authentication realm.

Field	Description
<b>Authentication Realm</b>	

Field	Description
Realm Type	Type of authentication realm: <ul style="list-style-type: none"> <li>Database - See <a href="#">Administrator Server Database Authentication Realm</a></li> <li>LDAP - See <a href="#">Administrator Server LDAP Authentication Realm</a></li> </ul> Default: Database.
<b>Superuser Credentials</b>	
Username	Name of the initial superuser. Default: root.
Password	Password of the superuser. Default: t. In the properties file, this value is obfuscated.

### Administrator Server Database Authentication Realm

If you select a database authentication realm, Administrator stores information about users and groups in a database. You can select the same database as the Administrator server, or configure a different database.

Field	Description
Use ActiveMatrix Administrator Server Database	Select if the database authentication realm should use the same database as the Administrator server. If cleared, the database configuration fields display. Default: Selected.

If you decide to use a non-default database, the wizard prompts you for database details.




Use the default embedded database only during development.


If you are using an external database, see [Database Requirements](#). To enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).



The properties that the wizard sets in the `build.properties` file depend on the context in which the prompts are displayed. By default, specify the properties for the Administrator Server database and the information is then used for the Notification Service database, the Log Service database, and the Payload Service database. You can, however, overwrite the values for the Notification Service, Log Service, and Payload Service, and you can change them in the `build.properties` file.



Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (postgresql-42.2.8.jar is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (postgresql-42.2.8.jar is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>
Database URL	<p>URL of the external database.</p> <p>Default: jdbc:hsqldb:hsq1://localhost:1234/amx.</p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the pg_hba.conf file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the pg_hba.conf file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: sa.</p>
Password	<p>External database password.</p> <p>Default: None.</p>
Max Connections	<p>Maximum number of database connections to allocate.</p> <p>Default: 10.</p>

Field	Description
Database Server is SSL Enabled	<p>Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.</p> <p>Default: Cleared.</p> <div>  <p>PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002.</p> </div>
Test Connection	Click the <b>Test Connection</b> button to ensure that you can connect to the database.

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	<p>Type of the keystore: JKS or JCEKS.</p> <p>Default: JKS.</p>
Keystore Password	Password that protects the keystore.

### Administrator Server LDAP Authentication Realm

If you select an LDAP authentication realm, Administrator stores information about users and groups in LDAP. You are prompted for the user and password, name resolution context, and server URLs. You can also specify the user search configuration and optional group information.

If you intend to enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).

Field	Description
Bind DN Name	<p>Distinguished name or name of the superuser to be used to connect to the server.</p> <p>Default: uid=Manager,ou=people,dc=example,dc=com.</p>
Password	<p>LDAP server password.</p> <p>Default: None.</p>

Field	Description
Context Factory	Factory object that provides the starting point for resolution of names within the LDAP server.  Default: com.sun.jndi.ldap.LdapCtxFactory
Machine Name Port List	Comma-separated list of URLs for an LDAP server. To achieve fault tolerance, you can specify multiple URLs. For example, server1.example.com:686, server2.example.com:1686.  Default: <i>machinename</i> :389, where <i>machinename</i> is the machine on which TIBCO Configuration Tool is being executed.
Fetch DN	You can retrieve the base DN (distinguished name) of the LDAP server.
<b>User Search Configuration</b>	
User Search Base DN (optional)	Base distinguished name from which the search starts.  Default: ou=people,ou=na,dc=example,dc=org
User Search Expression (optional)	Expression used for searching a user. For example: (CN=%U). '%U' is replaced by the username being searched for. You can define any complex filter such as (&cn=%U)(objectClass=account)).  Default: (&(uid={0})(objectclass=person)).
User Attribute with User Name (optional)	Name of the attribute in the user object that contains the user's name.  Default: uid.
Search Timeout (ms)	Time to wait for a response from the LDAP server. A values less than 90 seconds yields in a warning message.  Default: 30000.
Follow Referrals	Select to follow LDAP referrals. If you select this check box, requests to LDAP can be redirected to another server. Use this check box to indicate that the LDAP information might be available at another location, or possibly at another server or servers.  Ask your LDAP administrator whether LDAP referrals are used in your domain.

Field	Description
Group Indication (optional)	Specifies how a user's group memberships are found. Administrator uses group information when a user, once authenticated, performs other activities in the system. Options: <ul style="list-style-type: none"> <li><b>Group has users</b> - List of users that belong to the group. When selected, the Group Attribute with User Names field is enabled.</li> <li><b>User has groups</b> - List of groups to which the user belongs. When selected, the User Attribute with Group Names field is enabled.</li> </ul> Default: Group has users.

Field	Description
Group Search Base DN (optional)	Base distinguished name from which the search for the group starts. Default: ou=groups,ou=na,dc=example,dc=org.
Group Search Expression (optional)	Search by matching this expression against potential groups. Default: (&(cn={0})(objectClass=groupofuniqueNames)).
Group Attribute with User Names (optional)	Name of the attribute in the group object containing its users. Example: uniqueMember (OpenLDAP) or member (ActiveDirectory). Default: uniqueMember.
Group Attribute with Group Name (optional)	Name of the attribute in the group object that contains the name of the group. Example: cn (OpenLDAP) or sAMAccountName (ActiveDirectory). Default: cn.
Group Attribute Subgroup Names (optional)	Name of the attribute in the group object that contains its subgroups. Example: uniqueMember (OpenLDAP) or member (ActiveDirectory). Default: uniqueMember.
User Attribute with Group Names	Name of the attribute in the user object that lists the groups to which the user belongs. Default: None.
Group Search Scope Subtree	When searching the group, indicate whether to traverse into the subtree or to search only under the group base distinguished name. Default: Selected.

Field	Description
<b>LDAP Realm</b>	
User Search Scope Subtree	Select to have the search include the entire subtree starting at the base DN. Otherwise, search only the nodes one level below the base DN. Default: Selected.
Security Authentication	Value of Simple Authentication and Security Layer (SASL) authentication protocol to use. Values are implementation-dependent. Some possible values are simple, none, strong. Default: simple.
<b>LDAP Authentication</b>	
LDAP Server is SSL Enabled	Select to enable the LDAP server for SSL. When selected, the SSL Keystore Configuration fields are enabled. Default: Cleared.

Field	Description
Test Connection	Click the <b>Test Connection</b> button to ensure that you can connect to the LDAP database.

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	<p>Type of the keystore: JKS or JCEKS.</p> <p>Default: JKS.</p>
Keystore Password	Password that protects the keystore.

### Administrator Server TIBCO Credential Server Details

You can specify credential server details to identify the TIBCO Credential Server that you want to use with your Administrator server installation.

Field	Description
Network Adapter	<p>Address of the network adapter on the machine on which TIBCO Credential Server runs. The default is set to 0.0.0.0 so that TIBCO Credential Server will listen on all network adapters (including http://localhost and http://hostname). With the default setting, clients can connect to TIBCO Credential Server using any of the conventions (localhost, IP address, hostname). The value of this property must either be a hostname resolvable through DNS or 0.0.0.0; it cannot be an IP address.</p> <p>Default: 0.0.0.0.</p>
Port	<p>Management port number of the node, SystemNode, that runs TIBCO Credential Server.</p> <p>Default: 6041.</p>
Username	<p>User identifier for TIBCO Credential Server clients.</p> <p>Default: user1.</p>
Password	Password for the client.

## Administrator Server TIBCO Credential Server Keystore

If you enable SSL, you can use Administrator server with an auto-generated keystore or specify keystore information.

Field	Description
Auto-generated Keystore	Select to generate a TIBCO Credential Server keystore will be generated. When selected, the Common Name field displays. Default: Selected.
Common Name	Issuer name of TIBCO Credential Server. Default: amxadmin.
Provided Keystore	Check to provide TIBCO Credential Server keystore information. When selected, the keystore fields display. Default: Cleared.
Keystore Location	Location of the keystore.
Keystore Type	Type of keystore. Default: Autodetect.
Keystore Password	Password for the keystore.
Fetch Keystore	When you click this button, you can select one of the available key aliases, specify the keystore password, and click <b>Verify Keystore</b> to verify that the password you entered is valid.
Key Alias	Name of the alias used to access the identity
Key Password	Password for the alias

## Administrator Server Log Service Database

A log service is a TIBCO ActiveMatrix application that offers logging services. The log service application is deployed in the environment SystemEnvironment on SystemNode, the node that runs the Administrator server. A log service receives log entries sent to a JMS destination and stores the entries in a database.

If you did not deploy the logging and payload services when you created the Administrator server using the TIBCO Configuration Tool, see TIBCO\_HOME\administrator\version\scripts\logging\readme.txt.

Field	Description
Use ActiveMatrix Administrator Server Database	Select to have the log service use the same database as the Administrator server. If cleared, the database fields display. Default: Selected.

If you decide to use a non-default database, the wizard prompts you for database details.





Use the default embedded database only during development.

If you are using an external database, see [Database Requirements](#). To enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).



The properties that the wizard sets in the `build.properties` file depend on the context in which the prompts are displayed. By default, specify the properties for the Administrator Server database and the information is then used for the Notification Service database, the Log Service database, and the Payload Service database. You can, however, overwrite the values for the Notification Service, Log Service, and Payload Service, and you can change them in the `build.properties` file.

Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (<code>postgresql-42.2.8.jar</code> is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (<code>postgresql-42.2.8.jar</code> is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>
Database URL	<p>URL of the external database.</p> <p>Default: <code>jdbc:hsqldb:hsql://localhost:1234/amx.</code></p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the <code>pg_hba.conf</code> file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the <code>pg_hba.conf</code> file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: <code>sa</code>.</p>

Field	Description
Password	External database password. Default: None.
Max Connections	Maximum number of database connections to allocate. Default: 10.
Database Server is SSL Enabled	Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled. Default: Cleared.  <div>  PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002. </div>
Test Connection	Click the <b>Test Connection</b> button to ensure that you can connect to the database.

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.  <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS. Default: JKS.
Keystore Password	Password that protects the keystore.

### Administrator Server Payload Service Database

A payload service supports archiving, persisting and retrieving large size payload data. It is an independent service and does not depend on a log service. However, a log record sent to a log service can include a payload URL field to link a log message and payload data. You can store payload data in the same database used by Administrator server or use another database.

If you did not deploy the logging and payload services when you created the Administrator server using the TIBCO Configuration Tool, see *TIBCO\_HOME\administrator\version\scripts\logging\readme.txt*.



Field	Description
Use ActiveMatrix Administrator Server Database	Select to have the payload service use the same database as the Administrator server. If cleared, the database configuration fields display to let you specify database information.  Default: Selected.

If you decide to use a non-default database, the wizard prompts you for database details.





Use the default embedded database only during development.

If you are using an external database, see [Database Requirements](#). To enable SSL communications, see [Secure Communication Channels](#) and [SSL Requirements](#).



The properties that the wizard sets in the `build.properties` file depend on the context in which the prompts are displayed. By default, specify the properties for the Administrator Server database and the information is then used for the Notification Service database, the Log Service database, and the Payload Service database. You can, however, overwrite the values for the Notification Service, Log Service, and Payload Service, and you can change them in the `build.properties` file.

Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (<code>postgresql-42.2.8.jar</code> is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (<code>postgresql-42.2.8.jar</code> is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>

Field	Description
Database URL	<p>URL of the external database.</p> <p>Default: jdbc:hsqldb:hsq1://localhost:1234/amx.</p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the pg_hba.conf file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the pg_hba.conf file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: sa.</p>
Password	<p>External database password.</p> <p>Default: None.</p>
Max Connections	<p>Maximum number of database connections to allocate.</p> <p>Default: 10.</p>
Database Server is SSL Enabled	<p>Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.</p> <p>Default: Cleared.</p> <div>  <p>PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002.</p> </div>
Test Connection	<p>Click the <b>Test Connection</b> button to ensure that you can connect to the database.</p>

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	<p>Type of the keystore: JKS or JCEKS.</p> <p>Default: JKS.</p>
Keystore Password	Password that protects the keystore.

## Proxy Management Services Configuration

When you configure a TIBCO ActiveMatrix Policy Director Governance Administrator server, you are prompted for the proxy management services which include the default proxy URL pattern and, optionally, a node for proxy application deployment.

Field	Description
<b>Auto-generated Proxy URL default settings</b>	
Default proxy URL pattern	URL pattern for generated proxy applications. Options: <ul style="list-style-type: none"> <li>• <b>%Endpoint%</b> -</li> <li>• <b>%Endpoint%/proxy</b> -</li> <li>• <b>/proxy/%Endpoint%</b> -</li> </ul> Default: %Endpoint%
<b>Proxy Application deployment configuration</b>	
Create Node for Proxy Application Deployment	Check to set up a separate node for proxy application deployments. Default: Checked
Environment Name	Name of the new node's administrative domain. Default: DevEnvironment
Node Name	Name assigned to the new node. Default: ProxyNode
ActiveMatrix Host Name	Name of the TIBCO ActiveMatrix host on which the node you are creating will run. Default: SystemHost

## Summary

Each TIBCO Configuration Tool wizard's summary screen allows you to check the configuration that you specified and see the effects of that configuration. You can click Back to make changes, save the configuration for use by the silent installer, or click Configure to start the configuration. If you are using the console configuration tool, you can perform the same actions by typing single-letter commands, as prompted.

Field	Description
Session Scripts and Log Folder	The folder containing the script configured in the wizard and the log file if the script is executed.
Administrator URL	If an Administrator server was configured in the wizard, a link to the URL of the Administrator server.

Field	Description
Choose what you want to configure	Select the services you want to configure. Available options depend on choices you made earlier.
Select the products to deploy to nodes created in this session	Select the products to deploy. Available options depend on choices you made earlier.
Save	Saves the configuration in the location specified in the Session Scripts and Log Folder field.
Configure	Saves the configuration in the location specified in the Session Scripts and Log Folder field and performs the actions specified in Actions and Products to Deploy.
Cancel	Returns to the wizard selector screen.

## Create TIBCO ActiveMatrix Policy Director Governance Proxy Host

You can use a proxy host for use with your governance solution.

You can create a TIBCO ActiveMatrix Policy Director Governance Proxy Host instance using TIBCO ActiveMatrix Policy Director Governance Proxy Host Creation Wizard.

### TIBCO ActiveMatrix Policy Director Governance Proxy Host Creation Wizard

The ActiveMatrix Policy Director Governance Proxy Host creation wizard allows you to configure a proxy host. You can secure all communications with SSL if you want.

### TIBCO Host Selection

When you create a TIBCO ActiveMatrix Policy Director Governance Proxy Host, you can select an existing, preconfigured TIBCO Host to create the proxy host from, or create a proxy host from scratch.

Field	Description
<b>Select an existing TIBCO Host configuration</b>	
Allows you to create a proxy host by using the configuration of an already existing TIBCO host. Click <b>Next</b> to be prompted for information on the Proxy node and the transports for the proxy application.	
TIBCO Host configuration folder	Location of the configuration folder of the TIBCO Host for which you want to create a proxy host.  Each time you run TIBCO Configuration Tool, the first dialog prompts for a configuration folder.
Select configuration in chosen folder	Select the configuration in the folder you specified.
<b>Create a TIBCO ActiveMatrix Policy Director Governance Proxy Host</b>	
Allows you to create a proxy host from scratch. Click <b>Next</b> to be prompted for host configuration information.	

## TIBCO Host Instance

When you create a TIBCO Host instance, you are first prompted for the basic information that includes the name, enterprise and machine name, and behavior as a Windows application.

Field	Description
Name	Name of the TIBCO Host instance. The name must be unique within the enterprise. Default: None.
Enterprise Name	Name that defines a communication group for status messages sent between ActiveMatrix Administrator server and the hosts that are bound to the server. Default: amxadmin.
Machine Name	Name of the machine on which the TIBCO Host instance runs. Default: <i>hostname</i> , where <i>hostname</i> is the machine on which TIBCO Configuration Tool is being executed.
Management Port	Management port of the TIBCO Host instance. Default: 6001.
Register as Windows Service	Select to register the TIBCO Host instance as a Windows service named TIBCO ActiveMatrix <i>instanceName</i> , where <i>instanceName</i> is the name you specified in the Name field, with startup type Automatic. The service is not started. Default: Cleared.
Create Windows Shortcut	Select to create a shortcut named <i>instanceName</i> on the Windows desktop that points to <code>CONFIG_HOME\tibcohost\instanceName\host\bin\tibcohost.exe</code> and launches the TIBCO Host instance. Default: Cleared.

## TIBCO Host Instance Notification Server

When you create a standalone TIBCO Host instance, you can specify an associated notification server. This notification server can be the same server as that used by the Administrator, or you can define a different notification server.

The Notification Server is an Enterprise Message Service server that performs two essential system functions within the TIBCO ActiveMatrix platform. It delivers status messages sent by hosts and nodes to the Administrator server.

See [TIBCO Configuration Tool Requirements](#). If you intend to enable SSL communications, see [Secure Communication Channels](#).

Field	Description
Machine Name Port List	<p>Comma-separated list of <i>machinename:port</i> addresses for a TIBCO Enterprise Message Service (EMS) server.</p> <p>Default: <i>machinename:port</i>, where <i>machinename</i> is the host on which TIBCO Configuration Tool is being executed and <i>port</i> is 7222. The default <i>machinename:port</i> is <code>tcp://hostname:7222</code>. If the Enterprise Message Service server is SSL enabled, the hostname is <code>ssl://hostname:7222</code>.</p>
Username	<p>Username for the EMS server. The user must have administrator privileges in the EMS server. If the user does not have administrator privileges, configure your EMS server as described in <a href="#">Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users</a>.</p> <p>Default: admin.</p>
Password	<p>Password for the EMS user.</p> <p>Default: None.</p>
TIBCO Enterprise Message Service server is SSL enabled. Specify a trust store to establish trust with this server.	<p>Select to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.</p> <p>Default: Cleared.</p>

Field	Description
Create a Trust Store...	<p>Invokes a wizard to import certificates from a server and create the trust store.</p> <ol style="list-style-type: none"> <li>Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	<p>Type of the keystore: JKS or JCEKS.</p> <p>Default: JKS.</p>
Keystore Password	Password that protects the keystore.

Click **Test Connection** to verify that the keystore enables an SSL connection.

### TIBCO Host Instance Administrator Server

When you create a TIBCO Host instance, you can immediately bind it to an Administrator server and specify connection information for that server, or choose not to bind the TIBCO Host instance to an

Administrator server. You can assign the host to all environments. You can enable the connection for SSL.

Field	Description
Bind to Administrator Server	Select to bind the TIBCO Host instance to an Administrator server. When selected, the Administrator server configuration fields are enabled. Default: Selected.
Machine Name	Name of the machine on which the Administrator server is running. The value of this property must either be a hostname resolvable through DNS or 0.0.0.0 or IP address.
Port	Browser port used to access the Administrator server. Default: 8120.
Username	ID of the initial superuser. Default: root.
Password	Password of the superuser. Default: t.
Assign this Host to All Environments	By default, a host is assigned to all environments. Uncheck this check box to assign the host to no environment initially, and to explicitly assign the host to selected environments after configuration is complete.
Administrator Server is SSL Enabled	Select to enable the Administrator server internal port (see <a href="#">Administrator Server Internal HTTP Port</a> ) for SSL. When selected, the SSL Keystore Configuration fields are enabled.
Test connection	Click <b>Test Connection</b> to check whether the host can connect to the specified Administrator server.

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.  <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS. Default: JKS.

Field	Description
Keystore Password	Password that protects the keystore.

### Proxy Node Configuration

The Proxy Node Configuration screen allows you to specify the environment name, node name, and node management port for the proxy node associated with the proxy host.

Field	Description
<b>Auto-generated Proxy URL default settings</b>	
Default Proxy URL Pattern	URL pattern for generated proxy applications. Options: <ul style="list-style-type: none"> <li>• <b>%Endpoint%</b> -</li> <li>• <b>%Endpoint%/proxy</b> -</li> <li>• <b>/proxy/%Endpoint%</b> -</li> </ul> Default: %Endpoint%
<b>Proxy Node Configuration</b>	
Environment Name	Name of the environment that contains the node. Default: DevEnvironment
Node Name	Name of the proxy node you will create. Default: ProxyNode
Node Management Port	Management port of the node. Default: 4056
TIBCO ActiveMatrix Host	Name of the host you are creating and on which this node will run.

### TIBCO ActiveMatrix Policy Director Governance Proxy Host Configuration Summary

After you have made your selections in the Proxy Host wizard screens, the Summary screen allows you to select the parts of the configuration you want to perform. Click **Configure** after you have made your selection.

Field	Description
Sessions Scripts and Log Folder	Specify a folder for session logs and script files or accept the default.
Create TIBCO ActiveMatrix Policy Director Governance Proxy Host instance	Creates the proxy host instance, using the configuration information you just specified. Default: Checked



Field	Description
Launch TIBCO ActiveMatrix Policy Director Governance Proxy Host instance	Launches the proxy host instance after creation. Default: Checked
Register TIBCO ActiveMatrix Policy Director Governance Proxy Host instance to the Administrator server	Registers the proxy host instance Default: Checked
Create and configure TIBCO ActiveMatrix Policy Director Governance Proxy Node	Creates a node associated with the proxy host you are creating. Default: Checked

## Create TIBCO Host Instance

A TIBCO Host instance is one of the central components of any product in the TIBCO ActiveMatrix family of products. You can create an instance explicitly and give custom information about the instance, associated notification server, and associated Administrator server.



If you create a TIBCO Host instance, you cannot use that instance with an older version of the Administrator server.

Field	Description
Configure to Secure All Communication with SSL	Select to secure all communication channels with SSL. When you select this checkbox, the Enable SSL checkbox on the Notification and Messaging Bus Server and the ActiveMatrix Administrator server screens are selected. See <a href="#">Secure Communication Channels</a> for background information. Default: Cleared.

## TIBCO Host Instance

When you create a TIBCO Host instance, you are first prompted for the basic information that includes the name, enterprise and machine name, and behavior as a Windows application.

Field	Description
Name	Name of the TIBCO Host instance. The name must be unique within the enterprise. Default: None.
Enterprise Name	Name that defines a communication group for status messages sent between ActiveMatrix Administrator server and the hosts that are bound to the server. Default: amxadmin.
Machine Name	Name of the machine on which the TIBCO Host instance runs. Default: <i>hostname</i> , where <i>hostname</i> is the machine on which TIBCO Configuration Tool is being executed.

Field	Description
Management Port	Management port of the TIBCO Host instance. Default: 6001.
Register as Windows Service	Select to register the TIBCO Host instance as a Windows service named TIBCO ActiveMatrix <i>instanceName</i> , where <i>instanceName</i> is the name you specified in the Name field, with startup type Automatic. The service is not started. Default: Cleared.
Create Windows Shortcut	Select to create a shortcut named <i>instanceName</i> on the Windows desktop that points to <code>CONFIG_HOME\tibcohost\instanceName\host\bin\tibcohost.exe</code> and launches the TIBCO Host instance. Default: Cleared.

### TIBCO Host Instance Notification Server

When you create a standalone TIBCO Host instance, you can specify an associated notification server. This notification server can be the same server as that used by the Administrator, or you can define a different notification server.

The Notification Server is an Enterprise Message Service server that performs two essential system functions within the TIBCO ActiveMatrix platform. It delivers status messages sent by hosts and nodes to the Administrator server.

See [TIBCO Configuration Tool Requirements](#). If you intend to enable SSL communications, see [Secure Communication Channels](#).

Field	Description
Machine Name Port List	Comma-separated list of <i>machinename:port</i> addresses for a TIBCO Enterprise Message Service (EMS) server.  Default: <i>machinename:port</i> , where <i>machinename</i> is the host on which TIBCO Configuration Tool is being executed and <i>port</i> is 7222. The default <i>machinename:port</i> is <code>tcp://hostname:7222</code> . If the Enterprise Message Service server is SSL enabled, the hostname is <code>ssl://hostname:7222</code> .
Username	Username for the EMS server. The user must have administrator privileges in the EMS server. If the user does not have administrator privileges, configure your EMS server as described in <a href="#">Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users</a> . Default: admin.
Password	Password for the EMS user. Default: None.

Field	Description
TIBCO Enterprise Message Service server is SSL enabled. Specify a trust store to establish trust with this server.	Select to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.  Default: Cleared.

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.  1. Specify a password to protect the trust keystore and click <b>Next</b> . The SSL setup wizard displays certificates imported from the trusted server.  2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b> .
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS.  Default: JKS.
Keystore Password	Password that protects the keystore.

Click **Test Connection** to verify that the keystore enables an SSL connection.

### TIBCO Host Instance Administrator Server

When you create a TIBCO Host instance, you can immediately bind it to an Administrator server and specify connection information for that server, or choose not to bind the TIBCO Host instance to an Administrator server. You can assign the host to all environments. You can enable the connection for SSL.

Field	Description
Bind to Administrator Server	Select to bind the TIBCO Host instance to an Administrator server. When selected, the Administrator server configuration fields are enabled.  Default: Selected.
Machine Name	Name of the machine on which the Administrator server is running. The value of this property must either be a hostname resolvable through DNS or 0.0.0.0 or IP address.
Port	Browser port used to access the Administrator server.  Default: 8120.

Field	Description
Username	ID of the initial superuser. Default: root.
Password	Password of the superuser. Default: t.
Assign this Host to All Environments	By default, a host is assigned to all environments. Uncheck this check box to assign the host to no environment initially, and to explicitly assign the host to selected environments after configuration is complete.
Administrator Server is SSL Enabled	Select to enable the Administrator server internal port (see <a href="#">Administrator Server Internal HTTP Port</a> ) for SSL. When selected, the SSL Keystore Configuration fields are enabled.
Test connection	Click <b>Test Connection</b> to check whether the host can connect to the specified Administrator server.

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.  1. Specify a password to protect the trust keystore and click <b>Next</b> . The SSL setup wizard displays certificates imported from the trusted server.  2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b> .
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS. Default: JKS.
Keystore Password	Password that protects the keystore.

## Summary

Each TIBCO Configuration Tool wizard's summary screen allows you to check the configuration that you specified and see the effects of that configuration. You can click **Back** to make changes, save the configuration for use by the silent installer, or click **Configure** to start the configuration. If you are using the console configuration tool, you can perform the same actions by typing single-letter commands, as prompted.

The Summary screen displays the following information:

Field	Description
Session Script and Log Folder	Folder containing the script configured in the wizard and the log file if the script is executed.
Create TIBCO Instance	Select this option to create a TIBCO instance.
Launch TIBCO Instance	Select this option to launch a TIBCO instance.
Register TIBCO Instance to the Administrator Server	Select this option to register a TIBCO instance with the Administrator server.

## Configure Third-Party Driver

You can package a third-party driver into a feature and upload the feature with the Configure Third-Party Driver wizard. After the feature has been uploaded, you can add it to a node.

When you select the Configure Third-Party Driver wizard, you are prompted for information about the driver itself and for the driver JAR files.

### Third-Party Driver Details

The third-party driver details screen is used to provide detailed information about the driver you want to add to Administrator and install on nodes in your environment.

Field	Description
Driver Type	Type of driver being configured: JDBC, JMS, SiteMinder. Default: JDBC.

Field	Description
Driver	<p>Supported drivers:</p> <ul style="list-style-type: none"> <li>• <b>JDBC</b> <ul style="list-style-type: none"> <li>– TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>– TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>– TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>– TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>– TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>– TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>– TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>– TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>– TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>– TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>– TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>– TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>– TIBCO enabled JDBC driver for PostgreSQL 10.7.0 ( postgresql-42.2.8.jar is required)</li> <li>– TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (postgresql-42.2.8.jar is required)</li> </ul> </li> <li>• <b>JMS</b> <ul style="list-style-type: none"> <li>– TIBCO enabled JMS client for Sonic 6.1.0</li> <li>– TIBCO enabled JMS client for WebSphere 7.0.0. Support for WebSphere 6.0 is based on the backward compatibility of the WebSphere 7.0 client library. When a JMS binding is configured with JMS topics and needs to work with WebSphere 6.0, you must provide the WebSphere 7.0.1.3 version of the client library.</li> <li>– TIBCO enabled JMS client for WebSphere 7.5.0.  IBM MQ 8.0 is supported using the WebSphere 7.5.0 version of the client library.</li> </ul> </li> <li>• <b>SiteMinder</b> <ul style="list-style-type: none"> <li>– TIBCO-enabled SiteMinder SDK libraries for SiteMinder Agent 6.0.0</li> <li>– TIBCO-enabled SiteMinder SDK libraries for SiteMinder Agent 12.0.0</li> </ul> </li> </ul>

### Third-Party Driver JAR Folder

When you configure a third-party driver or other feature, you are prompted for the folder that contains the JARs to deploy to the Administrator server.

Field	Description
JAR Folder source.jar.folders	Folder containing the driver JARs to deploy to the Administrator server.

### Third-Party Driver Summary

After all your selections, the Third-Party Driver Summary page is displayed.

Field	Description
Sessions Scripts and Log Folder	Specify a folder for session logs and script files or accept the default.
Configure Third-Party Driver	Select this option to configure the third-part driver. Click <b>Save</b> to save the configuration.

### Edit ActiveMatrix Administrator Server Configuration

You can edit some aspects of the configuration for an existing Administrator server with TIBCO Configuration Tool.

This section describes the process of updating configuration settings that were initially specified when creating the Administrator server using TIBCO Configuration Tool.

To edit an existing configuration, follow these steps:

1. Start TIBCO Configuration Tool.
2. Select a `CONFIG_HOME` location for the Administrator server that you want to change.
3. Click **Edit TIBCO ActiveMatrix Administrator Server Configuration - V3.4**

Field	Description
Select server configuration	Select an Administrator server configuration from the drop-down list.

### Edit Administrator Server Configuration


You can edit the connection settings, database settings, or authentication realm settings for your Administrator server.

Field	Description
Edit HTTP Connection Settings	Edit the connection settings for the ActiveMatrix Administrator server.

Field	Description
Edit Database Settings	Edit the configuration details for the ActiveMatrix Administrator database.
Edit Authentication Realm Settings	Edit the configuration details for the Administrator authentication realm.

### Administrator Server Connection Settings

When you edit the connection settings, you can specify the network adapter and external port or enable SSL for HTTP communications. If you enable SSL, you are prompted to specify the certificate information. The defaults this screen displays show the current configuration settings.

Field	Description
Network Adapter	Address of the network adapter on the machine on which the Administrator server runs. The default is set to 0.0.0.0 so that Administrator will listen on all network adapters (including http://localhost and http://hostname). If you leave the default, clients can connect to the Administrator server using any of the conventions (localhost, IP address, hostname). The value of this property must either be a hostname resolvable through DNS or 0.0.0.0; it cannot be an IP address.
External HTTP Port	Port on which the Administrator clients access the Administrator server.
Enable SSL for External HTTP Port	Select to secure communication between Administrator server and clients with SSL. When selected, the Self-Signed Certificate and Imported Certificate radio buttons display.
Self-Signed Certificate	Indicate that the Administrator server will identify itself to clients with a self-signed certificate. When selected it uses the self signed certificate from the samples folder.   Do not use a self-signed certificate in production environments.
Imported Certificate	Indicate that Administrator server will identify itself to clients with a certificate imported into Administrator server. When selected, the Keystore fields and Fetch Keystore button are enabled.
Keystore Location	Location of the keystore to import.
Keystore Type	Type of keystore.
Keystore Password	Password that protects the keystore.
Fetch Keystore	When you click this button, you can select one of the available key aliases, specify the keystore password, and click Verify Keystore to verify that the password you entered is valid.



## Edit Administrator Server Database Details

The Edit Administrator Server Database Details screens is used to change the database details for your server. Using the wizard requires that you prepare your environment and that you perform some post-processing steps.

### Changing Database Details

To change the database details, perform the following steps:

1. From the TIBCO Administrator user interface, stop the following applications from the System environment:
  - com.tibco.amx.commonlogging.logservice.app
  - com.tibco.amx.commonlogging.payloadservice.app
2. Perform the following steps to uninstall the resource instances:
  - a. Make sure that you uninstall Log Service and Payload Service first. (TIBCO ActiveMatrix Payload Service Teneo Resource, TIBCO ActiveMatrix Log Service Teneo Resource).
  - b. Uninstall the Teneo resource instances from the system node (TIBCO ActiveMatrix Governance Teneo Resource).
  - c. Uninstall the Hibernate Resource Instance from the system node (TIBCO ActiveMatrix Governance Hibernate Resource).
  - d. Uninstall in the following order : Log Service or Payload Service in any order followed by the Governance JDBC shared resource instances from the system node. Ensure that the Governance JDBC shared resource instance must be the last to be uninstalled. It is recommended to use the Force Uninstall option for JDBC Resource Instance.




If you skip steps 3 to 7, please restart TIBCO Host manually.


3. If required, change the configuration of the user or database.
4. Start TIBCO Configuration Tool and select **Edit TIBCO ActiveMatrix Administrator Server Configuration - V3.4**.
5. Select the enterprise name and server name from the Server Configuration drop down menu, and select **Edit Database settings**.
6. Edit the database configuration, and click **Configure**.  
When update is complete, TIBCO Configuration Tool restarts the SystemNode node.
7. When the SystemNode node becomes available, log in to the TIBCO Administrator GUI and update the Governance JDBC resource with the new database configuration information. Cancel the pop-up to automatically synchronize the resource instances and applications.
8. Install the following:
  - a. JDBC Resource Instance for Governance JDBC Resource Instance. Make sure that Governance Service is installed before installing Log Service and Payload Service.
  - b. Install the Hibernate Resource Instance (TIBCO ActiveMatrix Governance Hibernate Resource).
  - c. Install the Teneo Resource Instances. Make sure Governance Service is done before installation of Log Service and Payload Service.



If the data base URL is changed to point to a different database, make sure you migrate all the data from the old database location to the new database location. Editing the configuration alone does not migrate the data.

Field	Description
Use Default In-Process Database	This will be checked if the current administrator uses an in-process database. TCT does not support editing the in-process database details.

Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (postgresql-42.2.8.jar is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (postgresql-42.2.8.jar is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>
Database URL	<p>URL of the external database.</p> <p>Default: jdbc:hsqldb:hsq://localhost:1234/amx.</p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the pg_hba.conf file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the pg_hba.conf file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: sa.</p>
Password	<p>External database password.</p> <p>Default: None.</p>
Max Connections	<p>Maximum number of database connections to allocate.</p> <p>Default: 10.</p>

Field	Description
Database Server is SSL Enabled	<p>Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.</p> <p>Default: Cleared.</p> <div>  <p>PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002.</p> </div>

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS.
Keystore Password	Password that protects the keystore.



If ActiveMatrix Administrator is not starting due to database connection failure, refer to the resolution listed in the *Troubleshooting* section of the *TIBCO ActiveMatrix® Service Grid Installation* guide.

### Changing ActiveMatrix Policy Director Governance Database Details



If you are using a common database for ActiveMatrix and ActiveMatrix Policy Director Governance, use the above procedure to change the database details.

If you are using a separate database for ActiveMatrix Policy Director Governance than the ActiveMatrix database, use the following steps to change the database details:

- From the TIBCO Administrator user interface, stop the following applications:
  - `com.tibco.amx.commonlogging.logservice.app`
  - `com.tibco.amx.commonlogging.payloadservice.app`
  - `com.tibco.amx.mcr.aggregator`
  - `com.tibco.ampd.ogp.de`
  - `com.tibco.ampd.psm`
- If required, change the configuration of the user or database.
- Make the appropriate changes to the TIBCO ActiveMatrix Governance JDBC Resource Shared Resource Template.
- Click **Cancel** on the pop-up.
- Install the JDBC Resource Instance for Governance JDBC Resource Instance. If the pop-up appears at this step, clear the selected applications. This automatically reinstalls Teneo and Hibernate Resource instances. If the pop-up does not appear, make sure that Teneo and Hibernate resource instances that were uninstalled in previous steps are installed now, and are in the Running state.

6. Manually install the JDBC, Teneo, and Hibernate resource instances by navigating to the **Resource Instance** tab for the JDBC shared resource. It automatically re-installs the Teneo and Hibernate shared resources.
7. After the resource installation is complete, restart TIBCO Host.
8. Restart the applications stopped in Step 1.

## Making Planned Database Configuration Changes

This section lists the steps to update the database configuration in a planned manner when you have the ActiveMatrix Administrator running.

### Procedure

1. Edit the JDBC resource templates and reinstall resource instances using the following steps:
  - a) In ActiveMatrix Administrator GUI, navigate to **Shared Objects > Resource Templates**.
  - b) **Select TIBCO ActiveMatrix PayloadService JDBC Resource.**

If you upgraded from a prior release, select **payloadJdbcSharedResource**.
  - c) In the Details section, update the database configuration and click **Save**. However, in the Apply Changes in Resource Template to Runtime window, click **Cancel**.
  - d) In the Resource Instances tab of the Details section, verify that the resource instance shows **Out of Sync**.
  - e) Click the **Install** button.
  - f) Wait and refresh till the status of the resource instance switches to **Running** and **In Sync**.
2. Repeat step 1, but for the resource templates -**TIBCO ActiveMatrix LogService JDBC Resource** and **TIBCO ActiveMatrix Governance JDBC Resource**. The order is important, and the TIBCO ActiveMatrix Governance JDBC Resource must be the last one.
 

If you upgraded from a prior release, select **cl\_logservice\_jdbc** and **GovernanceJDBCSharedResource**.
3. Make the planned database configuration change on the database server. For example, changing the password.
4. Using TIBCO Configuration Tool, update the database configuration for the ActiveMatrix Administrator as follows:
  - a) Select **Edit TIBCO ActiveMatrix Administrator Server Configuration**.
  - b) From the Select Server Configuration drop-down list, select the enterprise name and server name.
  - c) Check **Edit Database Settings**.
  - d) If the users or groups are defined in the Administrator database and not in an LDAP server, select **Edit Authentication Realm Settings**.
  - e) Click **Test Connection** to verify the settings.
  - f) Click **Configure** to apply the changes. When the update is complete, TIBCO Configuration Tool restarts the system node.
  - g) Wait for a few minutes for the system node to become available.

### Result

After the restart, the new database settings are fully in effect.

## Edit Administrator Server Authentication Realm

Administrator stores information about users and groups in an authentication realm. When you edit the Authentication realm, you can change the settings of the current realm, switch from a database to

LDAP, or switch from LDAP to a database. TIBCO Configuration Tool will then prompt you for more information about the authentication realm.

### Changing from a Database Realm to LDAP

Before you can change from a database realm to the LDAP realm, you have to add a new user in the current DB realm and assign the user as superuser. This new user must already be a user in the LDAP realm you want to use. See the *Administration* document for more information.

If you are changing from a Database realm to an LDAP realm, super user credentials are displayed. You need to enter the super user credentials you just created.

Enter the information about the authentication realm in the wizard screen.

### Changing from LDAP to a Database Realm

What happens when you change from LDAP to a database realm depends on whether the database realm is empty or not.

- If the new database realm is empty that is if it does not have any users in it, Administrator creates a new user called `tibco_user` with a password 't'.  
For this case, use the `tibco_user` superuser to log in to TIBCO Administrator after you have changed to a database realm and change the password. Consider creating a new superuser and deleting the default `tibco_user` user.
- If the new DB realm is not empty and does not contain any of the current superuser, a new user called `tibco_user` with password 't' is created.  
For this case, use the `tibco_user` superuser to log in to TIBCO Administrator after you have changed to a database realm and change the password. Consider creating a new superuser and deleting the default `tibco_user` user.
- If the new DB realm already contains a superuser that is also a superuser in LDAP, you can use that superuser. Administrator does not create a new user.

Enter the information about the authentication realm in the wizard screen.

Field	Description
<b>Authentication Realm</b>	
Realm Type	Type of authentication realm: <ul style="list-style-type: none"> <li>• Database - See <a href="#">Administrator Server Database Authentication Realm</a></li> <li>• LDAP - See <a href="#">Administrator Server LDAP Authentication Realm</a></li> </ul>
<b>Superuser Credentials</b>	
Username	Name of the initial superuser. Default: root.
Password	Password of the superuser. Default: t. In the properties file, this value is obfuscated.

## Edit Server LDAP Authentication Realm

If you select an LDAP authentication realm, Administrator stores information about users and groups in LDAP. You are prompted for the user and password, name resolution context, and server URLs. You can also specify the user search configuration and optional group information.

Field	Description
Bind DN Name	Distinguished name or name of the superuser to be used to connect to the server. Default: uid=Manager,ou=people,dc=example,dc=com.
Password	LDAP server password. Default: None.
Context Factory	Factory object that provides the starting point for resolution of names within the LDAP server. Default: com.sun.jndi.ldap.LdapCtxFactory
Machine Name Port List	Comma-separated list of URLs for an LDAP server. To achieve fault tolerance, you can specify multiple URLs. For example, server1.example.com:686, server2.example.com:1686. Default: <i>machinename</i> :389, where <i>machinename</i> is the machine on which TIBCO Configuration Tool is being executed.
Fetch DN	You can retrieve the base DN (distinguished name) of the LDAP server.
<b>User Search Configuration</b>	
User Search Base DN (optional)	Base distinguished name from which the search starts. Default: ou=people,ou=na,dc=example,dc=org
User Search Expression (optional)	Expression used for searching a user. For example: (CN=%U). '%U' is replaced by the username being searched for. You can define any complex filter such as (&cn=%U)(objectClass=account)). Default: (&(uid={0})(objectclass=person)).
User Attribute with User Name (optional)	Name of the attribute in the user object that contains the user's name. Default: uid.
Search Timeout (ms)	Time to wait for a response from the LDAP server. A values less than 90 seconds yields in a warning message. Default: 30000.

Field	Description
Follow Referrals	<p>Select to follow LDAP referrals. If you select this check box, requests to LDAP can be redirected to another server. Use this check box to indicate that the LDAP information might be available at another location, or possibly at another server or servers.</p> <p>Ask your LDAP administrator whether LDAP referrals are used in your domain.</p>

Field	Description
Group Indication (optional)	<p>Specifies how a user's group memberships are found. Administrator uses group information when a user, once authenticated, performs other activities in the system. Options:</p> <ul style="list-style-type: none"> <li>• <b>Group has users</b> - List of users that belong to the group. When selected, the Group Attribute with User Names field is enabled.</li> <li>• <b>User has groups</b> - List of groups to which the user belongs. When selected, the User Attribute with Group Names field is enabled.</li> </ul> <p>Default: Group has users.</p>
Group Search Base DN (optional)	<p>Base distinguished name from which the search for the group starts.</p> <p>Default: ou=groups,ou=na,dc=example,dc=org.</p>
Group Search Expression (optional)	<p>Search by matching this expression against potential groups.</p> <p>Default: cn={0}.</p>
Group Attribute with User Names (optional)	<p>Name of the attribute in the group object containing its users.</p> <p>Example: uniqueMember (OpenLDAP) or member (ActiveDirectory).</p> <p>Default: uniqueMember.</p>
Group Attribute with Group Name (optional)	<p>Name of the attribute in the group object that contains the name of the group.</p> <p>Example: cn (OpenLDAP) or sAMAccountName (ActiveDirectory).</p> <p>Default: cn.</p>
Group Attribute Subgroup Names (optional)	<p>Name of the attribute in the group object that contains its subgroups.</p> <p>Example: uniqueMember (OpenLDAP) or member (ActiveDirectory).</p> <p>Default: uniqueMember.</p>
User Attribute with Group Names	<p>Name of the attribute in the user object that lists the groups to which the user belongs.</p> <p>Default: None.</p>
Group Search Scope Subtree	<p>When searching the group, indicate whether to traverse into the subtree or to search only under the group base distinguished name.</p> <p>Default: Selected.</p>

Field	Description
<b>LDAP Realm</b>	
User Search Scope Subtree	Select to have the search include the entire subtree starting at the base DN. Otherwise, search only the nodes one level below the base DN.  Default: Selected.
Security Authentication	Value of Simple Authentication and Security Layer (SASL) authentication protocol to use. Values are implementation-dependent. Some possible values are simple, none, md-5.  Default: simple.
<b>LDAP Authentication</b>	
User DN Template (optional)	Template by which the User DN, used to connect to the LDAP server, is generated. Because the full DN is always supplied, the template should always be 0 (zero).  Default: uid={0},ou=people,ou=na,dc=org.
User Attributes Extra (optional)	Optional list of user attributes to retrieve from the LDAP directory during authentication.  Default: Empty (no additional attributes will be retrieved for the user).
LDAP Server is SSL Enabled	Select to enable the LDAP server for SSL. When selected, the SSL Keystore Configuration fields are enabled.  Default: Cleared.

## Summary

With each TIBCO Configuration Tool wizard's summary screen, you can check the configuration that you specified and see the effects of that configuration. You can click **Back** to make changes, save the configuration for use by the silent installer, or click **Configure** to start the configuration. If you are using the console configuration tool, you can perform the same actions by typing single-letter commands, as prompted.

When you edit the server configuration, the tasks you can perform depend entirely on selections made during configuration.

## Replicate TIBCO ActiveMatrix Administrator Server

In a production environment, you can set up your system to include a replica Administrator server on a second machine. Requests can be processed by either server. If one server is unavailable, the other server can process requests.

### Overview

You can replicate an Administrator server on a second machine by running TIBCO Configuration Tool. Before you run the TIBCO Configuration Tool wizard that performs replication, you must set up the source environment and the destination requirement.



## Shared File System Requirements and Overview

TIBCO Configuration Tool needs only read or write access for the shared file system. However, you should use a highly available filesystem in production environments. Consider using a SAN (storage area network) solution for shared folders and files. Place the TIBCO Administrator database on the SAN as well. Your storage needs depend on the number of DAA files you upload, on the number of application instances in use, and on the number of nodes you deploy the applications to.

After setup of the replica server, TIBCO Administrator reads from or writes to the shared file system each time it performs one of the following tasks:

- Lifecycle action for an application, such as create, delete, deploy, undeploy, start, stop, or upload DAA files.
- Lifecycle action for resource instances (installation)
- Changes to node features or logging configuration
- Startup of a runtime node

In a steady state, when no deployment is being performed and the applications are running, TIBCO Administrator does not read from or write to the shared filesystem.

If the shared file system is not available while deploying, the deployment task fails. To recover, retry the task. If you are using a SAN solution, this problem does not occur; only a highly available storage solution supports high availability for replicated TIBCO Administrator server setups.

## Setting Up Your Environment for Replication

Before you run TIBCO Configuration Tool for replication, you must set up your environment.

1. Install and configure Ant on both machines.
2. Set up an external database and use TIBCO Configuration Tool to configure the third-party driver for the corresponding database.
3. Set up a shared network drive on each machine. The shared network location must be the same on both machines. For example, if you create a network drive or folder on Machine 1 and map it to x: / shared , the shared drive or folder must be mapped to x: / shared as well.

On Windows 7 and Windows 2008, if you run the ActiveMatrix Administrator on a replicated setup as a Windows NT service:



- Ensure that you use the UNC path while setting up replication using TIBCO Configuration Tool.
- Also ensure that the "Log In" credentials for the Windows NT service is set to the credentials that were used to create the mapped drive.

**Machine 1** - Set up the first Administrator server on machine 1 by using the Create TIBCO ActiveMatrix Administrator Server wizard.

1. Install and configure your Administrator server and note down the following information.
  - *TIBCO\_HOME* location
  - *CONFIG\_HOME* location
  - Any passwords you provide.
2. On Machine 1, change the staging area folder location as follows.
  - a. Copy the folder *CONFIG\_HOME/admin/enterprise\_name/shared* to a location accessible from Machine 2.
  - b. To let the Administrator server on Machine 1 know about the new location of the shared folder, Open a command prompt at *TIBCO\_Home\administrator\3.4\scripts*.

- c. Run the following commands to update the folder information and restart the system node.
 

```
ant -f sharedWorkFolder_build.xml -Dadmin.shared.folder="NEW_SHARED_FOLDER_LOCATION"
-Dconfig.home="CONFIG_HOME" -Denterprise.name="ENTERPRISE_NAME"
```
- d. Restart the SystemNode node. From *CONFIG\_HOME/tibcohost/Admin-enterprise\_name-instance\_name/host/bin*, run the following commands.
 

```
tibcohost.exe stopNodes -nodeName SystemNode
tibcohost.exe startNodes -nodeName SystemNode
```

## Machine 2 - Replicate the Administrator server on Machine 2.

1. Run the installer, specifying the same *TIBCO\_HOME* location as Machine 1 is using.



If you want to install ActiveMatrix Policy Director Governance on replicated Administrator Server, select TIBCO ActiveMatrix PD installation profile while running the installer.

2. On Machine 1, copy the content of *CONFIG\_HOME/tct/keystore* and put it in the same folder on Machine 2. Create the folder if it does not exist.
3. Launch TIBCO Configuration Tool and select the same *CONFIG\_HOME* as was used on Machine 1.
4. Configure the same third-party driver as you did on Machine 1.
5. When TIBCO Configuration Tool returns to the wizard selection screen, click **Replicate TIBCO ActiveMatrix Administrator Server** and configure the replica server by responding to the wizard prompts.
  - a. In the Remote Administrator Details screen, enter the information to connect to the first Administrator server. This information is used to fetch the current configuration.
  - b. When you click **Next**, Machine 2 settings are validated. As part of validation, the wizard checks that.
    - Both machines use the same *CONFIG\_HOME*.
    - The shared folder is accessible and contains valid data.
    - The first administrator server is using an external database.
  - c. When validation is successful, you can provide a unique host name and node name for the replica server on the next screen.
 

The wizard displays the current Administrator server configuration. You cannot edit the configuration.
  - d. Enter passwords when prompted.
  - e. After entering the configuration details, click **Configure** to replicate the Administrator server.



After clicking **Configure** in TCT, in case any error occurs, user need to delete the partially installed replicated instance before starting over.



The TIBCO Configuration Tool Replicate TIBCO ActiveMatrix Administrator Server wizard does not show the configuration details for Monitoring, Logging, and Payload services. If those services are configured and deployed on the first Administrator server, they are automatically deployed on the replica server as part of the replication process.



While planning replication, ensure that both the Administrator servers have the same set of software versions including the hotfixes that were applied before upgrading to ActiveMatrix 3.4.0.

When you log in to one of the Administrator servers (or access the load balancing URL), you see the following system setup:

- Two hosts exist in the **Infrastructure > Hosts** screen.
- Two nodes exist in the SystemEnvironment environment in the **Infrastructure > Nodes** screen.

After completing the setup, requests can be processed by either server. If one server is unavailable, the other server can process requests.

## Configuring ActiveMatrix Policy Director Governance on Replicated Administrator Server

### Prerequisites

1. Install TIBCO ActiveMatrix Policy Director Governance on both Primary and Replicated machines in the same <TIBCO\_HOME> as TIBCO ActiveMatrix Service Grid installation.
2. On the primary machine, run TIBCO Configuration Tool from <TIBCO\_HOME>/tct/<version>/bin to configure TIBCO ActiveMatrix Policy Director Governance using the existing TIBCO ActiveMatrix Administrator.

To deploy TIBCO ActiveMatrix Policy Director Governance components on the replicated Administrator server instance, perform the following steps using the UI of the replicated Administrator Server instance:

### Procedure

1. In the ActiveMatrix Administrator UI, click **Applications**. Select the **SystemEnvironment** from **Environment** drop-down.
2. Deploy the following ActiveMatrix Policy Director Governance applications:  

```
com.tibco.ampd.ogp.de
com.tibco.ampd.psm
```
3. Click the application specified above.
4. Click the **Distribution** tab.
5. Select SystemNodeReplica in **Available Nodes** and add to **Selected Nodes**. Click **Save and Deploy**. Resolve the missing Resource Instances if any and click **Deploy**.
6. Deploy the following Policy Director Governance Plug-ins on the Replicated Administrator:  

```
TIBCO ActiveMatrix Operations Governance Platform Administrator plug-in
TIBCO ActiveMatrix Administrator Governance Policy Director admin plug-in
```
7. Navigate to **Admin Configuration > Plug-ins**. Select the plug-ins specified above and click **Deploy**.
8. Restart Replicated Administrator Server.

### Remote Administrator Server Details

The Remote Administrator Server Details screen is used to specify the machine name and port for the primary server. You must also specify the username and password. If you configured the primary server with SSL, you must perform SSL configuration for the replica server as well.

Field	Description
Machine Name	Name of the machine on which the primary Administrator server runs. The value of this property must be a hostname resolvable through DNS or an IP address.
Port	Management port that the primary Administrator server is using. Default: 8120

Field	Description
Username	User name of the administrator of the primary Administrator server. This user must be a super user. This credential is used to access the first admin server to get the current configuration. Only super user is allowed to query the current configuration.  Default: root
Password	Specify the password of the administrator of the primary Administrator server.
Administrator server is SSL enabled	If the primary Administrator server is SSL enabled, select this check box so that TIBCO Configuration Tool uses SSL to connect to the primary Administrator server. If you select the check box, you are prompted for keystore configuration information.
Test Connection	Click this button to verify that TIBCO Configuration Tool can access the server you specified using the username and password you specified.

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.  <ol style="list-style-type: none"> <li>1. Specify a password to protect the trust keystore and click <b>Next</b>. The SSL setup wizard displays certificates imported from the trusted server.</li> <li>2. In the <b>Trusted Certificates</b> area, select the checkboxes next to the certificates to trust and click <b>Finish</b>.</li> </ol>
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS.  Default: JKS.
Keystore Password	Password that protects the keystore.

### Create Replicated Instance Validation Info

The Create Replicated Instance Wizard Validation Info screen appears only if your system setup meets all requirements.

The requirements are listed in [Setting Up Your Environment for Replication](#).

## Administrator Server Configuration Details

You must specify a host name and node name for your replica server.


Field	Description
Enterprise Name	Displays the enterprise name of the remote Administrator server. You cannot change the enterprise name; the remote server and the replica server must be in the same enterprise.
Host Name	Name of the SystemHost instance that will be associated with the replica server. The host name must be unique. You cannot use the name you used for the host associated with the remote Administrator server.  Default: SystemHostReplica
Node Name	Name of the SystemNode instance to be associated with the replica server. The node name must be unique. You cannot use the name you used for the node associated with the remote Administrator server.  Default: SystemNodeReplica

## Administrator Server TIBCO Host Configuration

As part of the replica server setup, specify the machine and port for the TIBCO host on which the replica server runs. This information is for the local machine, not the remote machine.

Field	Description
Machine	Machine on which the TIBCO Host instance runs.
Port	Port for the TIBCO Host instance to communicate with other services in the environment.
Register as Windows Service	Select to register the TIBCO Host instance as a Windows service named TIBCO ActiveMatrix Admin-enterpriseName-serverName with startup type Automatic. The service is not started.  Default: Cleared.
Create Windows Shortcut	Select to add a shortcut named TIBCO ActiveMatrix Admin - enterpriseName -serverName that points to CONFIG_HOME\tibcohost\Admin-enterpriseName-serverName\host\bin\tibcohost.exe to the Windows desktop.  Default: Cleared.



## Administrator Server Connection Settings

Field	Description
Network Adapter	Address of the network adapter on the machine on which the Administrator server runs. The default is set to 0.0.0.0 so that Administrator listens on all network adapters (including http://localhost and http://hostname). If you leave the default, clients can connect to the Administrator server using any of the conventions (localhost, IP address, hostname). The value of this property must either be a hostname resolvable through DNS or 0.0.0.0; it cannot be an IP address.
Management Port	Management port of the node that runs Administrator server. Default: 6021.
External HTTP Port	Port on which Administrator clients access the Administrator server. Default: 8120.
Enable SSL for External HTTP Port	Select to secure communication between the Administrator server and clients with SSL. When selected, the Self-Signed Certificate and Imported Certificate radio buttons display. Default: Same as for remote server.
Self-Signed Certificate	Indicates that the Administrator server identifies itself to clients with a self-signed certificate generated by <a href="#">TIBCO Credential Server</a> .  Do not use a self-signed certificate in production environments. Default: Same as for remote server.
Imported Certificate	Indicates that the Administrator server identifies itself to clients with a certificate imported into the Administrator server. When selected, the Keystore fields and Fetch Keystore button are enabled.
Keystore Location	Location of the keystore to import.
Keystore Type	Type of keystore.
Keystore Password	Password that protects the keystore.
Fetch Keystore	When you click this button, you can select one of the available key aliases, specify the keystore password, and click Verify Keystore to verify that the password you entered is valid.

## Administrator Server Notification and Messaging Bus Server

The notification server is an Enterprise Message Service server that delivers status messages sent by hosts and nodes to the Administrator server.


Click **Test Connection** to make sure that you can connect to EMS from the replica administrator machine.

Field	Description
Machine Name Port List	<p>Comma-separated list of <i>machinename:port</i> addresses for a TIBCO Enterprise Message Service (EMS) server.</p> <p>Default: <i>machinename:port</i>, where <i>machinename</i> is the host on which TIBCO Configuration Tool is being executed and <i>port</i> is 7222. The default <i>machinename:port</i> is <code>tcp://hostname:7222</code>. If the Enterprise Message Service server is SSL enabled, the hostname is <code>ssl://hostname:7222</code>.</p>
Username	<p>Username for the EMS server. The user must have administrator privileges in the EMS server. If the user does not have administrator privileges, configure your EMS server as described in <a href="#">Configuring TIBCO Enterprise Message Service Servers for Non-Admin Users</a>.</p> <p>Default: admin.</p>
Password	<p>Password for the EMS user.</p> <p>Default: None.</p>
TIBCO Enterprise Message Service server is SSL enabled. Specify a trust store to establish trust with this server.	<p>Select to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.</p> <p>Default: Cleared.</p>
No Messaging Bus	<p>See <a href="#">Determining Whether an Enterprise Needs a Messaging Bus</a>.</p> <p>Select to create an enterprise that does not use a messaging bus. This is useful in scenarios where you do not want to distribute applications and hence do not need a messaging bus. In such scenarios, applications can be deployed even if the messaging bus is down or not available.</p> <ul style="list-style-type: none"> <li>• If <b>No Messaging Bus</b> is selected, it creates an enterprise that does not use a messaging bus.</li> </ul> <div>  <p>Do not use select this checkbox if you are setting up TIBCO ActiveMatrix BPM. It could result in the failure of the TIBCO ActiveMatrix BPM setup.</p> </div> <ul style="list-style-type: none"> <li>• If <b>No Messaging Bus</b> is cleared, it creates an enterprise that uses a messaging bus. You can then choose to create an environment with or without a messaging bus.</li> </ul> <div>  <p>Even if <b>No Messaging Bus</b> is cleared and you create an enterprise that uses the messaging bus, you can later configure the enterprise to stop using a messaging bus. For more information, see section "Configuring an Enterprise to Stop Using a Messaging Bus" of <i>TIBCO ActiveMatrix Service Grid Administration Guide</i>.</p> </div> <p>Default: Cleared.</p> <p>For more information on how to configure messaging bus settings related to an environment, see <i>TIBCO ActiveMatrix Service Grid Administration Guide</i>.</p>


## Administration Server Database Details

The administrator server that you are replicating must be set up to use an external database. This screen displays the information about the external database used by the first admin server. You cannot change this information for the replica server.

Click Test Connection to make sure you can connect to the database from the replica machine.

Field	Description
Database Driver	<p>Driver for the external database:</p> <ul style="list-style-type: none"> <li>• TIBCO enabled JDBC driver for IBM DB2 4.12.55</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.19.66</li> <li>• TIBCO enabled JDBC driver for IBM DB2 4.24.92</li> <li>• TIBCO enabled JDBC driver for Oracle 11.1.0</li> <li>• TIBCO enabled JDBC driver for Oracle 12.1.100</li> <li>• TIBCO enabled JDBC driver for Oracle 12.2.0</li> <li>• TIBCO enabled JDBC driver for Oracle 18.3.0</li> <li>• TIBCO enabled JDBC driver for Oracle 19.3.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 4.2.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 6.0.0</li> <li>• TIBCO enabled JDBC driver for Microsoft SQL Server 7.0.0</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 10.7.0 (postgresql-42.2.8.jar is required)</li> <li>• TIBCO enabled JDBC driver for PostgreSQL 11.5.0 (postgresql-42.2.8.jar is required)</li> </ul> <p>Default: JDBC driver provided for HSQL 1.8.400.</p>
Database URL	<p>URL of the external database.</p> <p>Default: jdbc:hsqldb:hsqldb://localhost:1234/amx.</p> <div>  <p>For PostgreSQL database, you must add client machine IP address entry in the pg_hba.conf file. If the TIBCO ActiveMatrix Administrator is replicated, you must also add IP address of the machine on which ActiveMatrix Administrator is replicated in the pg_hba.conf file. For more information, see PostgreSQL documentation.</p> </div>
Username	<p>External database username.</p> <p>Default: sa.</p>
Password	<p>External database password.</p> <p>Default: None.</p>



Field	Description
Max Connections	Maximum number of database connections to allocate. Default: 10.
Database Server is SSL Enabled	Select to enable the database server for SSL. When selected, the SSL Keystore Configuration fields are enabled. Default: Cleared.  PostgreSQL database with SSL enabled is not supported in TIBCO ActiveMatrix 3.4.0 Hotfix 002.

### Administrator Server Database Authentication Realm Details

If you selected a database authentication realm on the remote server, both Administrator server instances will store information about users and groups in a database. This screen displays connection information for the database you set up from the remote server.

You can review connection information in this screen, then enter the password for the specified database and click **Test Connection**.

### Administrator Server Configuration LDAP Authentication Realm

If you select an LDAP authentication realm when you configure the remote Administrator server, Administrator retrieves information about users and groups from LDAP. This screen shows the LDAP configuration used by the first administrator server.

Click the **Test Connection** button to make sure the connection between LDAP server and the replica server works properly.

### Administrator Server Configuration Summary

Each TIBCO Configuration Tool wizard's summary screen allows you to check the configuration that you specified and see the effects of that configuration. You can click **Back** to make changes, save the configuration for use by the silent installer, or click **Configure** to start the configuration. If you are using the console configuration tool, you can perform the same actions by typing single-letter commands, as prompted.

The Administrator Server Configuration Summary screen displays information about the session scripts and log folder and about the Administrator URL. For this wizard, you can only choose to replicate the remote server, or cancel the replication.

### Deleting an Administrator Server

If you are using a replica Administrator server, the TIBCO Configuration Tool wizard does not allow you to delete a replica instance, if you want to. You can delete from the command line.

#### Prerequisites

Make sure that the super user specified in the `remote_props.properties` has `force_delete` permission. Only users with explicit `force_delete` and super user permission are allowed to delete the Administrator server instance.



Do not run the deletion script on the machine on which the Administrator instance you want to delete is running. For example, assume your cluster consists of Administrator instance A running on machine X and Administrator instance B running on machine Y. To delete instance B, run the script from instance A running on machine X.

## Procedure

1. Open a command window.
2. Go to the following directory.  
`CONFIG_HOME/admin/enterprise_name/samples`
3. Edit the `deleteAdminInstance_data.xml` file to update the node and host name properties.
4. Run the following command.  
**ant -f deleteAdminInstance\_build.xml**  
When you run this command, the replica node is deleted from the environment and the replica host will be unregistered. If the replica host has any runtime nodes, the replica host is not unregistered.
5. If the replica host is unregistered, go to the machine on which the administrator instance was running and terminate the TIBCO Host process.

## Upgrade or Downgrade TIBCO ActiveMatrix

You can upgrade or downgrade an existing ActiveMatrix Administrator server, runtime hosts and nodes using the Upgrade or Downgrade TIBCO ActiveMatrix wizard. To upgrade or downgrade:

1. Start the TIBCO Configuration Tool.
2. Select whether you want to upgrade or downgrade.
3. Select the hosts that you want to upgrade or downgrade. TIBCO Configuration Tool runs some diagnostic tests for the selected host and recommends whether the host is eligible for upgrade or downgrade or not. It also generates reports. Refer to the [Diagnostic Tests](#) section for more details.
4. Select from the following actions, as appropriate, in the Summary Screen:
  - Stop hosts before proceeding with the upgrade or downgrade
  - Upgrade or downgrade selected hosts
  - Perform post-upgrade tasks (only for upgrade)
  - Restart hosts after a successful upgrade or downgrade
5. Click **Upgrade** or **Downgrade** in the last screen of TIBCO Configuration Tool to perform the selected actions.

## Upgrade or Downgrade

You can upgrade or downgrade an existing ActiveMatrix Administrator server, runtime hosts and nodes using the Upgrade or Downgrade TIBCO ActiveMatrix wizard.

The following table lists the options available in the wizard.

Field	Description
Upgrade	Upgrade to TIBCO ActiveMatrix 3.4.0. It validates the specified CONFIG_HOME and then upgrades all Hosts or a selection of Hosts to 3.4.0.
Downgrade	Downgrade from TIBCO ActiveMatrix 3.4.0. It validates the specified CONFIG_HOME and then downgrades all Hosts or a selection of Hosts from 3.4.0.

## Upgrade Options

The following table lists the options available while upgrading hosts using the Upgrade or Downgrade TIBCO ActiveMatrix wizard.

Field	Description
Upgrade All TIBCOHosts	Upgrades all the hosts in the specified CONFIG_HOME to 3.4.0.
Select TIBCOHosts to be upgraded	Upgrades selected hosts in the specified CONFIG_HOME to 3.4.0.
Skip diagnostic tests (not recommended)	Skips the validation of specified CONFIG_HOME.

## Upgrade Selection

If you choose to upgrade only selected hosts, the following table lists the options that are available during the selection of the hosts.

Field	Description
Select TIBCOHosts to be upgraded	Upgrades selected hosts in the specified CONFIG_HOME to 3.4.0.
Skip diagnostic tests (not recommended)	Skips the validation of the specified CONFIG_HOME.

## Validate

TIBCO Configuration Tool runs diagnostic tests to find out if there are any issues with the specified CONFIG\_HOME that might prevent a successful upgrade or downgrade process.

Field	Description
Results of diagnostic tests	Results of the diagnostic tests are displayed in this area.
Eligibility of CONFIG_HOME	<ul style="list-style-type: none"> <li>• ELIGIBLE: Indicates that the diagnostic tests were successful and that the specified CONFIG_HOME is eligible for the upgrade or downgrade process.</li> <li>• NOT ELIGIBLE: Indicates that some of the diagnostic tests failed and that the specified CONFIG_HOME is not eligible for the upgrade or downgrade process.</li> </ul>
Rerun tests	Allows you to run the diagnostic tests again.
Diagnostic report	Opens a text version of the complete diagnostic report.





For more information on the diagnostic tests, refer to [Diagnostic Tests](#).



Sometimes, even when a host is not eligible for a downgrade, the **Next** button on the Validate screen is enabled and the console returns a SUCCESS message. The TIBCO Configuration Tool does not FAIL when the upgrade for a particular node or host is skipped, even though the upgrade for other TIBCO hosts and nodes has passed.

## Upgrade Summary

The Upgrade Summary provides a summary of selections and actions that will be performed during the upgrade. The following table lists the options available on the Upgrade Summary screen.

Field	Description
Session Scripts and Log Folder	Folder where the scripts and logs for the current session are stored.
Stop All or Selected TIBCO Hosts	<p>Stops all or selected hosts and nodes managed by the hosts (including manual nodes) before proceeding with the upgrade.</p> <p> Nodes are stopped irrespective of the startup mode.</p>
Upgrade All or Selected TIBCO Hosts	<p>Upgrades all or selected hosts.</p> <p> All nodes managed by the hosts are upgraded automatically.</p>
Perform post-upgrade tasks	<p>Performs the post-upgrade task after a successful upgrade.</p> <p> This task is recommended when upgrading a system host (ActiveMatrix Administrator nodes).</p>
Start All or Selected TIBCO Hosts	<p>Re-starts all or selected hosts after a successful upgrade.</p> <p> Nodes are stopped irrespective of the startup mode.</p>
Upgrade	<p>Depending on the check boxes selected, clicking on <b>Upgrade</b>, performs the tasks in the following order:</p> <ol style="list-style-type: none"> <li>1. Stops all or selected hosts.</li> <li>2. Upgrades all or selected hosts to 3.4.0.</li> <li>3. Performs a post-upgrade task.</li> <li>4. Re-starts all or selected hosts.</li> </ol> <p>If an action is completed and it was successful, <b>(c)</b> is displayed beside it.</p> <p>If an action is completed but with an error, <b>(f)</b> is displayed beside it.</p> <p>If an action was aborted because one of the previous actions failed, <b>(a)</b> is displayed beside it.</p>
Details	As upgrade might take time, if you want to see the current status of tasks, click <b>Details</b> to see more information.

## Downgrade Options

The following table lists the options available while downgrading hosts using the Upgrade or Downgrade TIBCO ActiveMatrix wizard.

Field	Description
Downgrade All TIBCOHosts	Downgrades all the hosts in the specified CONFIG_HOME.
Select TIBCOHosts to be downgraded	Downgrades selected hosts in the specified CONFIG_HOME.
Skip diagnostic tests (not recommended)	Skips the validation of the specified CONFIG_HOME.

## Downgrade Selection

If you choose to downgrade only selected hosts, the following table lists the options that are available during the selection of the hosts.

Field	Description
Select TIBCOHosts to be downgraded	Downgrades selected hosts in the specified CONFIG_HOME.
Skip diagnostic tests (not recommended)	Skips the validation of the specified CONFIG_HOME.



## ActiveMatrix Administrator Server

The following table lists the ActiveMatrix Administrator server details that need to be specified while upgrading or downgrading an ActiveMatrix Administrator server using the wizard.

Field	Description
Machine name	The machine on which the ActiveMatrix Administrator Server exists.
Port	Port used to connect to the server.
Username	User name for the server.
Password	Password for the user.
Admin server is SSL enabled. Use the trust store below to establish trust with the server.	<p>Select this check box if the server is SSL-enabled.</p> <p>When checked, the SSL Keystore configuration fields are enabled.</p> <p>Default: Unchecked.</p>

## Downgrade Summary

The Downgrade Summary provides a summary of selections and actions that will be performed during the downgrade. The following table lists the options available on the Downgrade Summary screen.

Field	Description
Session Scripts and Log Folder	Folder where the scripts and logs for the current session are stored.
Stop All or Selected TIBCO Hosts	<p>Stops all or selected hosts and nodes managed by the hosts (including manual nodes) before proceeding with the downgrade.</p> <p> Nodes are stopped irrespective of the startup mode.</p>
Downgrade All or Selected TIBCO Hosts	<p>Downgrades all or selected hosts.</p> <p> All nodes managed by the hosts are downgraded automatically.</p>
Start All or Selected TIBCO Hosts	Re-starts all or selected hosts after a successful downgrade.
Downgrade	<p>Depending on the check boxes selected, clicking on <b>Downgrade</b>, performs tasks in the following order:</p> <ol style="list-style-type: none"> <li>1. Stops all or selected hosts.</li> <li>2. Downgrades all or selected hosts.</li> <li>3. Re-starts all or selected hosts.</li> </ol> <p>If an action is completed and it was successful, <b>(c)</b> is displayed beside it.</p> <p>If an action is completed but with an error, <b>(f)</b> is displayed beside it.</p> <p>If an action was aborted because one of the previous actions failed, <b>(a)</b> is displayed beside it.</p>
Details	As downgrade might take some time, if you want to see the current status of tasks, click <b>Details</b> to see more information.

## Update JRE used by TIBCO ActiveMatrix

Updates the TIBCO\_HOME (and all CONFIG\_HOMEs using the TIBCO\_HOME) to use the specified JRE version.



Before updating the JRE version, you must shutdown the Host instance you are managing to avoid errors.

### Select JRE Home

1. Select the folder that contains JRE.



Provide the JRE\_HOME (and not the JDK\_HOME) bundled inside the JDK.

2. Select the Java Home location of the JRE version that you would like to use.

### Summary

The Summary screen provides a summary of selections and actions that can be performed during the JRE update.

Field	Description
Session Scripts and Log Folder	Location of the configuration folder where the session details and log files are stored. You can accept the default or click <b>Browse</b> to specify a new location.
Update	Updates the JRE for a given TIBCO_HOME and all the "TIBCO ActiveMatrix Administrator Instances" referencing it.
Dry Run	Displays information on what would have been done if the command was executed. The actual command is not executed.
Save	Saves the configuration.

Click **Configure** to update the specified TIBCO\_HOME to the specified JRE\_HOME path.



While configuring JRE for ActiveMatrix Service Grid 3.4 version, in the **Update JRE used by TIBCO ActiveMatrix v3.4** screen, specify the path as C:\Program Files\Java\jre1.8.0\_181 and click **Update**. It updates the JRE version successfully. If an error is displayed, run the command two or three times until it succeeds.

## Configure TIBCO Service Performance Manager

Start TIBCO Configuration Tool from TIBCO\_HOME/tct/<version>/TIBCOConfigurationTool and select **Configure TIBCO Service Performance Manager - V2.3** from the first screen. The TIBCO Configuration Tool screens guide you to configure various details such as database configuration, JMS configuration, threadpool configuration, and so on.

### TIBCO Service Performance Manager Configuration: Database Configuration

The following table lists the database configuration details that can be configured using the wizard.

#### *Database Configuration Properties*

Field Name	Property in spm-config. properties	Mandatory	Default Value	Description
Database Driver	rtajdbc.driver	Yes	org.postgresql.Driver	Name of the JDBC Driver.  Supported values are oracle.jdbc.driver.OracleDriver, com.microsoft.sqlserver.jdbc, SQLServerDriver, and com.ibm.db2.jcc.DB2Driver.

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Database URL	rtajdbc.url	Yes	jdbc:postgresql://localhost:5432/<database>	Location of the database server.  See the documentation specific to your JDBC driver for more information.
Username	rtajdbc.user	Yes	spm_user	Username that the Service Performance Manager server uses to access the database.  This user must have read and write permissions to the database.
Password	rtajdbc.password	Yes		Password that the server uses, in conjunction with the username provided in dbstore_driver_username, to access the database.

Select **Advanced Options** to configure advanced database options.



If you do not select **Advanced Options**, the advanced properties take default values. However, if you use **Advanced Options**, the properties take the last configured values.

#### *Database Configuration Advanced Properties*

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Initial Connections	rtajdbc.initial.connection.size	No	10	Number of connections allowed at initialization.
Max Connections	rtajdbc.max.connection.size	No	100	Maximum number of simultaneous client connections to the database.
Transaction Batch Size	rtajdbc.batch.size	No	1000	Database batch size.
JDBC Key	rtajdbc.key	No	""	Database connection pool internal identifier.

To test the validity of the database connection:



1. For the database that you choose, make the jar files of the drivers available and specify the complete path of the jar file in the **JDBC Driver Path** field.
2. Click **Test Connection**.

## JMS Configuration

The following table lists the JMS configuration details that can be configured using the wizard.

### *JMS Configuration Properties*

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Context Factory	rtajms.jndi.contextfactory	No	com.tibco.tibjms.naming.TibjmsInitialContextFactory	JMS Transport JNDI context factory
Provider URL	rtajms.jndi.url	No	tibjmsnaming://localhost:7222	JMS provider URL
Username	rtajms.connection.username	No	admin	JMS provider connection username.
Password	rtajms.connection.password	No	The default value is the obfuscated value of <BLANK>. Note that it is not a single blank space character.	JMS provider connection password.

Select **Advanced Options** to configure advanced JMS options.



If you do not select **Advanced Options**, the advanced properties take default values. However, if you use **Advanced Options**, the properties take the last configured values.

### *JMS Configuration Advanced Properties*

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Queue Connection Factory	rtajms.queueconnectionfactory	No	SPMQueueConnectionFactory	JMS queue connection factory
Inbound Queue	rtajms.inbound.queue	No	spm.inbound.queue	JMS inbound queue for the Service Performance Manager server to receive messages

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Outbound Queue	rta.jms.outbound.queue	No	spm.outbound.queue	JMS outbound queue for the Service Performance Manager server to send messages
Inbound Query Queue	rta.jms.inbound.query.queue	No	spm.inbound.query.queue	JMS inbound query queue for Service Performance Manager server to receive messages.
Fault Tolerance Queue	rta.ft.queue.name	No	spm.ft.queue	This is the queue on which the Service Performance Manager server exchanges messages related to fault tolerance. The Service Performance Manager Client API does not use this queue.
Retry Interval	rta.jms.connection.retry.interval	No	5000	JMS connection retry interval. Time interval in milliseconds for retrying a failed JMS connection.
Outbound Message Expiry	rta.jms.outbound.message.expiry	No	432000000	JMS message expiration in milliseconds for outbound messages from the Service Performance Manager server.

### Threadpool Configuration

The following table lists the threadpool configuration details that can be configured using the wizard.

#### *Threadpool Configuration Properties*

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Common Threadpool Size	rta.worker.thread.count	No	32	The number of worker threads for the common thread pool

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Metric Compute Threadpool Size	rta.metric.compute.thread.count	No	32	Number of threads to perform the core computation jobs. Each hierarchy computes on a single thread.

Select **Advanced Options** to configure advanced threadpool options.



If you do not select **Advanced Options**, the advanced properties take default values. However, if you use **Advanced Options**, the properties take the last configured values.

#### *Threadpool Configuration Advanced Properties*

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Common Threadpool Queue Size	rta.worker.queue.size	No	64	The queue size for the common thread pool
Metric Compute Threadpool Queue Size	rta.metric.compute.queue.size	No	64	Queue size for the metric thread pool. Change it only when you change rta.metric.compute.thread.count. A value twice the queue thread size is recommended.
Common Threadpool Minimum Threads	rta.worker.thread.count.min	No	0	The minimum number of threads to retain in the thread pools even when there is less load on them. This value should be less than or equal to rta.worker.thread.count.
Common Threadpool Idletimeout	rta.worker.thread.idle.timeout	No	300	Time interval in seconds after which idle threads of the thread pools are stopped, till the thread count reaches the rta.worker.thread.count.min setting.

## Server Configuration

The following table lists the server configuration details that can be configured using the wizard.

### Server Configuration Properties

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Schema Store Location	rta.schema.store	No	SPM_HOME/config	Location on the file system where the server loads the schema files.
L1 Cache Size	rta.l1.cache.size	No	10000	Size of the L1 cache used to store metric nodes. L1 cache ensures that frequently used data is cached inside the JVM and hence not loaded from the database. The L1 cache uses an LRU algorithm.

Select **Advanced Options** to configure advanced threadpool options.



If you do not select **Advanced Options**, the advanced properties take default values. However, if you use **Advanced Options**, the properties take the last configured values.

### Server Configuration Advanced Properties

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Server Batch Size	rta.server.batch.size	No	100	Client batches further are batched on the server for processing, for enhanced performance. This property specifies the batch size to use on the server.
Server Batch Size Flush Period (ms)	rta.server.batch.flush.period	No	5000	Time interval in milliseconds to wait for a server batch to complete. Incomplete batch is still processed at this interval.

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Rule Metric Node Cache Size	rta.l1.cache.size.rule.metric.nodes	No	10000	Size of the L1 cache used to store rule/action state nodes. Larger cache with appropriately large JVM heap (-Xmx setting) results in better performance.
Session Heartbeat Threshold (ms)	rta.config.session.heartbeat.threshold	No	60000	Maximum time in milliseconds that a named session can be kept alive, since the last heart beat from client is received.
Snapshot Query Timeout	rta.snapshot.query.timeout	No	300000	Defines timeout in milliseconds for expiration of snapshot query. If the query is not accessed for the specified duration, it expires after the specified period.
Rules Actions Scan Frequency	rta.rules.actions.scan.frequency	No	5000	Specifies in milliseconds how often to scan for scheduled actions,

### Storage and Recovery Configuration

The following table lists the storage and recovery details that can be configured using the wizard.

### Storage and Recovery Configuration Properties

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Store Facts	rta.store.facts	No	false	Whether to store the facts into the database. For a very high transaction rate, setting this property to <code>false</code> helps improve the performance.  Since Service Performance Manager 2.3.0 relies on EMS for recovery, it is not necessary to store these facts. One may still need to store them for business reasons.
Process Duplicate Facts	rta.process.duplicate.facts	No	true	Defines whether to process or skip duplicate facts. Applicable only when <code>rta.store.facts=true</code> . Else this has no effect.  When set to <code>true</code> , reprocess a possible duplicate fact.  When set to <code>false</code> , skip over a possible duplicate fact.

### Action Configuration

The following tables list the mail and log details that can be configured using the wizard.

#### Email Action Configuration Properties

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
SMTP Server Host	rta.mail.smtp.host	Yes	none	Used by E-mail alert actions. Specifies the SMTP server host name.
SMTP Server Port	rta.mail.smtp.port	No	25	Used by E-mail alert actions. SMTP server port.

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Authenticate SMTP Server	rta.mail.smtp.authentication	No	false	Used by E-mail alert actions. Specifies whether the SMTP server authentication is required or not.  The SMTP Server Username and SMTP Server Password fields are enabled if this check box is selected.
SMTP Server Username	rta.mail.smtp.user	No	none	Used by E-mail alert actions. Required only if SMTP server authentication is true. Specifies the SMTP server user name.
SMTP Server Password	rta.mail.smtp.password	No		Used by E-mail alert actions. Required only if SMTP server authentication is true. Specifies SMTP server user password.  You can also enter an encrypted password in this field. To encrypt the password, you can use a password generator tool to obfuscate it. If the password entered in the spm-config.properties file is plain-text, the same appears in the Configuration tab on TIBCO ActiveMatrix Dashboard.
Email Sender Address	rta.mail.from	No	Current system user	Used by E-mail alert actions. Specifies E-mail From (E-mail Sender)

Select **Advanced Options** to configure advanced threadpool options.



If you do not select **Advanced Options**, the advanced properties take default values. However, if you use **Advanced Options**, the properties take the last configured values.

### Email Action Advanced Configuration Properties

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Mail Retry Count	rta.mail.retry.count	No	3	This field is under Advanced Options. Maximum number of times to retry the send email operation. A value of -1 attempts this operation infinitely.
Mail Retry Interval	rta.mail.retry.interval	No	2000	This field is under Advanced Options. Time interval, in milliseconds, between retry attempts.

### Log Action Configuration Properties

Field Name	Property in spm-config.properties	Mandatory	Default Value	Description
Log Format	rta.log.alert.format	No	XML	The default format of logging actions is XML. As an alternate, you can use the TEXT format.

## Handle Configuration File

The following steps show how to handle configuration files:

### Starting Service Performance Manager with a TRA file

The Service Performance Manager server uses two different files, one for starting the server JVM and another for application configuration. `tibspm.tra` is the default file used to start the server JVM. This file provides runtime parameters to start the JVM, such as heap sizes, classpath, and so on. It also passes on the application specific configuration to the server using the `application_args` property. By default, this property points to `spm-config.properties` in `SPM_HOME/config` folder. You can use TIBCO Configuration Tool to change the `application_args` property to a different TRA file as follows:

In the **SPM Start TRA File** option, specify the full path of the new TRA file. Remember that the TRA file should first be created externally.



To start Service Performance Manager with the new TRA file, use `tibspm --propFile <new-tra-file>`.



## Changing or Overriding the Existing Server Configuration

### Save Options for the Configuration File

Option	Description
<b>Override the original configuration file</b>	Select this option to apply the current configuration to the existing server configuration file, which by default for the first time, is <code>spm-config.properties</code> in <code>SPM_HOME/config</code> folder.
<b>Save as a new file</b>	Select this option to create a new file with the specified name and location.

In both cases, the chosen TRA file is modified to use this server configuration by changing its `application_args` property accordingly.

TIBCO Configuration Tool also stores these changes such that the defaults values are loaded from the last run.



The default values are not be loaded from the last run if there is a previous version of TIBCO Configuration Tool installed in this `TIBCO_HOME` as part of another TIBCO product installation. If so, you must explicitly load the previously stored configuration using the "Load" option and point it to the appropriate sessions files.

### Summary Configuration

TIBCO Configuration Tool now shows the location of the folder where the current session state is stored. You can change it as required.

1. Select a location for the **Session Scripts and Log Folder**.
2. Ensure that **Configure TIBCO Service Performance Manager Arguments** is selected. It is selected by default.
3. Click **Configure** to configure the server.

### Generate TIBCO Service Performance Manager Database Schema

You can use TIBCO Configuration Tool to generate the database schema. Alternatively, you can use the `TIBCO_HOME/spm/<version>/bin/tibspmdlgenerator` utility from the command prompt to generate the Service Performance Manager database schema.

Provide the following details:

Item	Description
Database Type	The target database for which the database DDL schema files must be generated. Select one of the supported databases.
Config folder	Location of the Service Performance Manager schema XML files. By default, it is at <code>TIBCO_HOME/spm/&lt;version&gt;/config</code> .
Output Folder	The generated scripts are stored at this location. By default, it is at <code>TIBCO_HOME/spm/&lt;version&gt;/bin/&lt;Database_Type_Name&gt;</code> .

Item	Description
Property File	Default values for database output folders and so on are read from a property file. By default, it is at TIBCO_HOME/spm/<version>/bin/tibspmddlgenerator.tra.

Click **Generate Scripts** to generate the database schema. An information window indicating the successful creation of the schema is displayed. Click **OK**. In the Output folder location, the following files are generated:

```
spm_<database_type_name>_cleanupddl.sql
spm_<database_type_name>_createdddl.sql
spm_<database_type_name>_dropddl.sql
```

### Summary Configuration

TIBCO Configuration Tool now shows the location of the folder where the current session state is stored. You can change it as required.

1. Select a location for the **Session Scripts and Log Folder**.
2. Ensure that **Configure TIBCO Service Performance Manager Arguments** is selected. It is selected by default.
3. Click **Configure** to configure the server.

### Configure TIBCO Service Performance Manager Dashboard

Start TIBCO Configuration Tool from TIBCO\_HOME/tct/1.6/TIBCOConfigurationTool and select **Configure TIBCO ActiveMatrix SPM Dashboard - V3.4** from the first screen. The TIBCO Configuration Tool screens guide you to configure various details such as EMS server, authentication realm configuration, and so on.

### Generate Database Configuration

You can configure options related to generating database scripts.

### Database Configuration

The following table lists the database configuration details that can be configured using the wizard.

Field	Description
Database Driver	Driver for the external database.
Database URL	URL of the external database.
Username	External database username.
Password	External database password.
Max Connections	Maximum number of database connections to allocate.
Database Server is SSL Enabled	Check to enable the database server for SSL. When checked, the SSL Keystore Configuration fields are enabled.

When the **Database Server is SSL Enabled** field is checked, the following SSL Keystore Configuration fields are enabled.

Field	Description
Create a Trust Store...	Invokes a wizard to import certificates from a server and create the trust store.
Browse	Invokes a dialog to navigate to a keystore file.
Keystore Location	Location of the keystore.
Keystore Type	Type of the keystore: JKS or JCEKS. Default: JKS.
Keystore Password	Password that protects the keystore.

### JMS Configuration

The following table lists the JMS configuration details that can be configured using the wizard.

#### *TIBCO ActiveMatrix SPM Dashboard JMS Configuration Properties*

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
Context Factory	rta.client.jms.jndi.contextfactory	No	com.tibco.tibjms.naming.TibjmsInitialContextFactory	JMS JNDI context factory
Provider URL	rta.client.jms.jndi.url	No	tibjmsnaming://localhost:7222	JMS JNDI URI
Username	rta.client.connection.username	No	admin	Defines the Username for creating the RTA client session
Password	rta.client.connection.password	No		Defines the password for creating the RTA client session. This is obfuscated using the obfuscation utility that is shipped with the product.
Test Connection				Tests an EMS connection.

(Optional) Select **Advanced Options** to configure advanced JMS options. Provide the following values and click **Next**.



If you do not select **Advanced Options**, the advanced properties take default values. However, if you use **Advanced Options**, the properties take the last configured values. The `spmdashboard-config.properties` file has the last configured values.

### *TIBCO ActiveMatrix SPM Dashboard JMS Configuration Advanced Properties*

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
Queue Connection Factory	<code>rta.client.jms.queueconnectionfactory</code>	No	<code>SPMQueueConnectionFactory</code>	JMS queue connection factory
Inbound Queue	<code>rta.client.jms.inbound.queue</code>	No	<code>spm.inbound.queue</code>	The JMS queue on which the client API sends fact messages. It should match the server's <code>rta.jms.inbound.queue</code> property.
Inbound Query Queue	<code>rta.client.jms.inbound.query.queue</code>	No	<code>spm.inbound.query.queue</code>	The JMS queue to which the query or other synchronous request/reply-based messages are sent. It should match the server's <code>rta.jms.inbound.query.queue</code> property.
Outbound Queue	<code>rta.client.jms.outbound.queue</code>	No	<code>spm.outbound.queue</code>	The JMS queue to receive asynchronous messages like streaming query responses, alerts and server notifications. It should match the server's <code>rta.jms.outbound.queue</code> property.

### Threadpool Configuration

You can specify the Threadpool configuration for the ActiveMatrix SPM Dashboard.

### Server Configuration

You can configure properties related to the SPM Server.

### Storage And Recovery Configuration

You can specify how storage and recovery options for the ActiveMatrix SPM Dashboard are to be handled.

### Action Configuration

You can define the action you want the SPM Server to take if certain conditions are met. You can choose an email action, log action, or a custom action.

## Handle Configuration File

You can specify how the configuration files for ActiveMatrix SPM Dashboard are to be handled.

### Client API JMS Configuration

#### *TIBCO ActiveMatrix SPM Dashboard Client API JMS Configuration Properties*

Field Name	Default Value	Description
Context Factory	com.tibco.tibjms.naming.TibjmsInitialContextFactory	JMS Client API context factory
Provider URL	tibjmsnaming://localhost:7222	JMS Client API URI
Username	admin	Username for creating the Client session
Password		Defines the password for creating the Client session.  This is obfuscated using the obfuscation utility that is shipped with the product.

(Optional) Select **Advanced Options** to configure advanced Client API JMS options.

#### *TIBCO ActiveMatrix SPM Dashboard Client API JMS Advanced Properties*

Field Name	Default Value	Description
Queue Connection Factory	SPMQueueConnectionFactory	JMS Client API queue connection factory
Inbound Queue	spm.inbound.queue	The JMS Client API queue on which the client API sends fact messages. It should match the server's Inbound Queue property.
Inbound Query Queue	spm.inbound.query.queue	The JMS Client API queue to which the query or other synchronous request/reply-based messages are sent. It should match the server's Inbound Query Queue property.
Outbound Queue	spm.outbound.queue	The JMS Client API queue to receive asynchronous messages like streaming query responses, alerts and server notifications. It should match the server's Outbound Queue property.

Click **Test Connection** to test the connection to EMS.

## Client API Configuration

### *TIBCO ActiveMatrix SPM Dashboard Client API Configuration Properties*

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
Retry Count	rta.client.retry.count	No	10	Defines the client retry count for the failed JMS operations.

(Optional) Select **Advanced Options** to configure advanced Client API options.

### *TIBCO ActiveMatrix SPM Dashboard Client API Advanced Properties*

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
Retry Wait Interval (ms)	rta.client.retry.wait	No	10000	Retry interval in milliseconds for the rta.client.retry.count property.
Client Heartbeat Interval (ms)	rta.client.heartbeat.interval	No	10000	Time interval in milliseconds used by named client sessions to send heartbeats.
Client Sync Response Timeout	rta.client.sync.response.timeout	No	10000	Time interval in milliseconds for a client to wait for the server to send response for a sync operation such as, query registration before timing out the operation.
Client Async Dispatcher Max Pool Size	rta.client.async.dispatcher.max.pool.size	No	2147483647	The maximum number of threads of the asynchronous message dispatcher thread pool. This thread pool is used to dispatch asynchronous messages to the client API.
Client Async Dispatcher Timeout	rta.client.async.dispatcher.timeout	No	300000	The thread pool used for dispatching results from an outbound queue to clients has an idle timeout in milliseconds.

## Dashboard Server Configuration

### *TIBCO ActiveMatrix SPM Dashboard Server Configuration Properties*

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
Session Name	rta.client.connection.sessionname	No	DashBoard-session \$time\$	Defines the session name which is used to create the client session
Root Directory for Preference Storage	rta.mal.storage.file.root	No	TIBCO_HOME/config	Defines the root directory for file storage
Database Name for Preference Storage	rta.mal.storage.file.dbname	No	store	Defines the database name for file storage

(Optional) Select **Advanced Options** to configure advanced server options.

### *TIBCO ActiveMatrix SPM Dashboard Server Configuration Advanced Properties*

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
Token Timeout	rta.token.timeout	No	1800000	When a UI client authenticates with the TIBCO ActiveMatrix SPM Dashboard server, a token is issued to the user. All further communication between the UI client and the TIBCO ActiveMatrix SPM Dashboard server happens through the token validation.  This property defines the period of inactive time before a token is marked as timed out. The default is 30 minutes (1800000 milliseconds)
Snapshot Query Batch Size	rta.snapshot.query.batch.size	No	1000	Defines the batch size to use for snap shot queries

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
Streaming Query Batch Size	rta.streaming.query.batch.size	No	1	Defines the batch size to use for streaming queries
MAX Data Rows In Time Based Data Set	rta.max.timeresultset.fetch.count	No	1000	Defines the maximum amount of data rows that are fetched in a time-based data set. This is also applicable for alerts.
Alert Datetime Formats	rta.alerts.datetimeformats	No	yyyy-MM-dd'T'HH:mm:ss.SSZ	The date time format to be used for date time in alerts
Enable Dashboard Server Stats	rta.stats.enabled	No	true	Lists the dashboard server statistics.

### Dashboard Server Security Configuration

#### *TIBCO ActiveMatrix SPM Dashboard Security Configuration Properties*

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
Enable Default Principal	rta.enable.default.principal	No	false	Enables adding a default principal if the underlying security provider did not return any principals
Logging Configuration File (JAAS)	rta.java.security.auth.login.config	No	SPM_HOME/config/jaas-config.config	Defines the login configuration to be used by JAAS
Authentication Type	rta.auth.type	No	file	Determines which type of authentication to use. Possible values are <code>ldap</code> and <code>file</code> .

### Dashboard Server Authentication LDAP Configuration

#### *TIBCO ActiveMatrix SPM Dashboard LDAP Configuration Properties*

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
IsAnonymous	auth.ldap.isAnonymous	No	false	Allows you to log into LDAP anonymously



Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
UseRoleDN	rta.auth.ldap.useRoleDN	No	true	Decides whether to use role dn
LDAP Host	rta.auth.ldap.host	No		The name of the ldap host
LDAP Port	rta.auth.ldap.port	No		The port of the ldap host
Fetch DN				Retrieves the base DN (distinguished name) of the LDAP server.
LDAP Admin DN	rta.auth.ldap.adminDN	No		The admin user name for connecting to ldap
Admin Password	rta.auth.ldap.admin Password	No		The admin password for connecting to ldap
LDAP Base DN	rta.auth.ldap.baseDN	No		The base DN for the ldap
SearchExpression	(&uid={0})(objectclass=person))			Expression used for searching a user.
Ldap Uidattr	rta.auth.ldap.uidattr	No	uid	The ldap attribute to search username against
LDAP Object Class	rta.auth.ldap.objectClass	No	*	The ldap object to search for
LDAP Role Attr	rta.auth.ldap.roleAttr	No	nsroledn	Decides whether to use Role DN
LDAP DN Attr	rta.auth.ldap.dnAttr	No	distinguishedName	
Test Connection				Tests an LDAP connection.

### Tomcat Server Configuration

Enter **Tomcat Port**. By default, it is 8080.

## Dashboard Server Authentication File Configuration

### *TIBCO ActiveMatrix SPM Dashboard File Configuration Properties*

Field Name	Property in spmdashboard-config.properties	Mandatory	Default Value	Description
Authentication File Path	rta.auth.file.location	No	\$SPM_HOME/config/users.pwd	The location of the file which is to be used as the user database

### Summary Configuration

1. TIBCO Configuration Tool now shows the location of the folder where the current session state is stored, in the **Sessions Scripts and Log Folder**. You can change it as required.
2. Ensure that **Configure ActiveMatrix SPM Dashboard Server** is selected. It is selected by default.
3. Click **Configure** to configure the dashboard.

Alternatively, you can manually change the properties specified in the `SPM_HOME/config/spmdashboard-config.properties` file. If you do not want to use TIBCO Configuration Tool to configure the TIBCO ActiveMatrix SPM Dashboard, you can override any default value of a property from the `spmdashboard-config.properties` file.



TIBCO Configuration Tool does not recognize the changes made directly to the `spmdashboard-config.properties` file. Hence, it is recommended to always use TIBCO Configuration Tool to make changes to the configuration.

By default, TIBCO ActiveMatrix Dashboard listens on port 8080. You can change this number using TIBCO Configuration Tool. To manually change the port number:



1. Open the `SPM_HOME/amxdashboard/tomcat/conf/server.xml` file.
2. Change the port number in the following code snippet:

```
<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443" />
```

## DDL Script Generator

The DDL Script Generator is used to generate database specific DDL scripts defining the database schema needed to operate the ActiveMatrix Administrator server.

### Overview of the DDL Script Generator Utility

Use the DDL Script Generator utility to manually create the database schema.

By default, when you create an ActiveMatrix Administrator server using Tibco Configuration Tool, the database schema objects are created automatically when the ActiveMatrix Administrator server starts up the first time. If you do not want the software to automatically create the database schema objects at runtime, before creating the ActiveMatrix Administrator server, use the DDL Script Generator Utility. For a list of permissions needed to create the schema, see [Configuring External Databases](#). After this step, the database administrator (DBA) must execute the scripts to create the database schema objects that ActiveMatrix Administrator server needs.

The utility is used in the following two scenarios:

- While creating a new ActiveMatrix Administrator server, use the utility to generate scripts for creating the database schema.

- After deleting all ActiveMatrix Administrator server instances, while cleaning clean up a part or whole of an existing schema. The utility generates scripts to cleanup the database schema.

## Creating the Database Schema

You can explicitly generate DDL scripts and use them to create the database schema.

### Procedure

1. On the machine that runs ActiveMatrix Administrator, configure the drivers for database using TIBCO Configuration Tool.
2. Navigate to the *TIBCO\_HOME/administrator/<version>/samples/ddl* folder.
3. Edit the *generate\_ddl.xml* file and modify the *dbType* and *dialect* for your database type under the *create* target. See [DDLGeneratorTask](#) for more information.

```
<target name="create">
    <DDLGeneratorTask
        action="create"
        targetDirectory="${admin.ddl.samples.directory}"
        dbType="oracle11g"
        dialect="com.tibco.amf.sharedresource.runtime.core.hibernate.
            dialects.Oracle10gDialect" />
</target>
```



If you are creating the second instance of a replicated ActiveMatrix Administrator Server, skip steps 2 and 3 while creating the ActiveMatrix Administrator server.

4. Execute `ant -f generate_ddl.xml create`.
5. Ensure that the Database Prerequisites mentioned under [Configuring External Databases](#) are met. Have the DBA execute the script files - *create\_\*.ddl* in the corresponding databases as explained in the [Database Models](#) section.
6. (Optional) In addition to the generated scripts, if you want to use the Monitoring service, the DBA needs to execute an additional script corresponding to the monitoring data. It can be found under *<TIBCO\_HOME>/administrator/<version>/scripts/governance/ddl/create\_\*.sql*. Use the script corresponding to your database type.
7. Run TIBCO Configuration Tool again to create the ActiveMatrix Administrator server.

### Result

The DDL scripts are generated and can be used to execute on the database.

Sample DDLGeneratorTask element

## Cleaning up the Database Schema

Use the DDL Script Generator utility to generate scripts to clean up the database.

### Procedure

1. On the machine that runs ActiveMatrix Administrator, configure the drivers for database using TIBCO Configuration Tool.
2. Navigate to the *TIBCO\_HOME/administrator/<version>/samples/ddl* folder.
3. Edit the *generate\_ddl.xml* file and modify the *dbType* and *dialect* for your database type under the *drop* target. See [DDLGeneratorTask](#) for more information.

```
<target name="drop">
    <DDLGeneratorTask
        action="drop"
    />
</target>
```

```
targetDirectory="${admin.ddl.samples.directory}"
dbType="oracle11g"
dialect="com.tibco.amf.sharedresource.runtime.core.hibernate.
dialects.Oracle10gDialect" />
</target>
```

4. Execute `ant -f generate_ddl.xml drop`.
5. Depending on what portions of the schema you want to remove, have the DBA execute the script files - `drop_*.ddl` in the corresponding databases as explained in the [Database Models](#) section.
6. (Optional) In addition to the generated scripts, if you want to use the Monitoring service, the DBA needs to execute an additional script corresponding to the monitoring data. It can be found under `<TIBCO_HOME>/administrator/<version>/scripts/governance/ddl/drop_*.sql`. Use the script corresponding to your database type.

## Database Models

TIBCO Configuration Tool (TCT) allows you to configure separate databases for ActiveMatrix Administrator, Database realm, Common logging service and Monitoring service.

By default, the DDL Script Generator generates four separate scripts for each model:

Scripts	Description
admin	The database schema for the core functionality in ActiveMatrix Administrator
security	The database schema for Database authentication realm, specifically needed to store users and groups in the database (not applicable for LDAP)
commonlogging	The database schema that stores log and payload records created by the Common Logging service.
governance	The database schema that stores metadata used by the Monitoring service. The metadata has a separate schema than the actual monitoring data; although they can be in the same database.

By default, the DDL generator produces scripts for every model. Depending on which databases you want in each model, execute the script for that model in its corresponding database. You can skip one or more DDL scripts if you do not want to use that functionality for the model. For example, while using LDAP authentication realm you skip the DDL scripts for the security model.

The default name for DDL files is composed of `<action>_<model>.ddl` (where `<action>` is create, drop or update).

For example, `create_admin.ddl` is the schema creation script for the core functionality in ActiveMatrix Administrator. Similarly, `drop_admin.ddl` is the schema deletion script.

## DDLGeneratorTask

DDLGeneratorTask specifies an action, data and property files, the objects on which the action is performed, and various behavioral attributes.

```
<DDLGeneratorTask
  action="action"
  targetDirectory="path to the samples directory"
  targetFilePrefix="targetFilePrefix"
  modelProfiles="modelProfiles"
  dbType="dbtype"
  dialect="dialect"
  username="username"
  password="password"
  dbUrl="dbUrl" />
```

Attribute	Type	Req?	Description
action	String	Yes	<p>The action to be performed by the generated scripts.</p> <ul style="list-style-type: none"> <li>• create - scripts to create tables and related database objects are created.</li> <li>• drop - scripts to delete tables and related database objects.</li> </ul> <p>The action is case insensitive.</p>
targetDirectory	String	No	<p>The location of the directory where the generated scripts files are stored.</p> <p>Default: TIBCO_HOME/administrator/&lt;version&gt;/samples/ddl.</p>
targetFile	String	No	<p>The name of generated script file. the location of the script file. If specified, this attribute takes precedence over the targetDirectory attribute.</p>
targetFilePrefix	String	No	<p>The prefix for the generated scripts. Used only when the targetFilePrefix attribute is used.</p>
dbtype	String	No	<p>The database for which to generate the scripts. Valid values:</p> <ul style="list-style-type: none"> <li>• sqlserver</li> <li>• db2</li> <li>• oracle</li> </ul>
dialect	String	Yes	<p>The dialect of the specified database.</p>
username	String	No	<p>Used to connect to the database.</p>
password	String	No	<p>Used to connect to the database.</p> <p>The password for the specified username attribute can be either clear text or encrypted value.</p>
dburl	String	Yes	<p>Used to connect to the database.</p>

Attribute	Type	Req?	Description
modelProfiles	String	Yes	<p>Used to specify a model for which to generate the scripts. Multiple values can be specified using a comma-separated list.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• admin</li> <li>• governance</li> <li>• commonlogging</li> <li>• security</li> <li>• all - generate scripts for all the models listed above.</li> </ul>

## Configuring TIBCO Service Performance Manager Components

Configure the SPM server, SPM dashboard server, and SPM service probe as follows:

1. Set the EMS\_HOME for the SPM server and SPM dashboard, as described in [Setting EMS\\_HOME](#).
2. Create EMS queues and factories for the SPM server and SPM dashboard, as described in [Creating EMS Queues and Factories](#).
3. Set the properties for the SPM dashboard, as described in [Setting Properties for the SPM Dashboard](#).
4. Configure the SPM dashboard server to use the SPM Server, as described in [Configure the SPM Dashboard Server to use the SPM Server](#).
5. Configure the SPM dashboard server (EMS server, authentication realm configuration, and so on), as described in [Configure TIBCO Service Performance Manager Dashboard](#).
6. Configure the SPM server, as described in [Configuring the TIBCO Service Performance Manager Server](#).
7. Generate the database schema and start the database, as described in [Generating the Database Schema and Starting the Database](#).
8. Enable the SPM service probe for SystemNode and DevNode, as described in [Enabling the Service Probe using TIBCO ActiveMatrix Administrator UI](#) or [Enabling the Service Probe Using TIBCO ActiveMatrix Administrator CLI](#).
9. Start the TIBCO SPM server by executing `TIBCO_HOME/spm/2.3/bin/tibspm.exe`.
10. Start the TIBCO SPM dashboard by executing `TIBCO_HOME/amxspmdashboard/3.4/amxdashboard/startamxdashboard.bat`.
11. Restart the TIBCOHost.
12. Access `http://localhost:8080/amxdashboard/` for testing the ActiveMatrix SPM dashboard. Use the Admin/Admin credentials.
13. (Optional) Change the heap size of the SPM server, as described in [Changing the Heap Size of the Server](#).
14. (Optional) Change the logging configuration of the [SPM server](#), [SPM dashboard](#), or the [SPM example](#) as required.

## Setting EMS\_HOME


For Service Performance Manager, you must set the *EMS\_HOME* and create EMS queues and factories. Based on the location of the EMS server and the SPM server, you must manually set the *EMS\_HOME*.

These steps depend on:

- The installation order of TIBCO Enterprise Message Service and TIBCO Service Performance Manager
- Whether they share the same *TIBCO\_HOME* or use a different *TIBCO\_HOME*
- Whether they are installed on the same machine or on different machines

The following table covers the scenarios and corresponding steps.

Setup Details	Installation Order	Steps
Single machine with the same <i>TIBCO_HOME</i>	<ol style="list-style-type: none"> <li>1. TIBCO Enterprise Message Service</li> <li>2. TIBCO Service Performance Manager</li> </ol>	No manual steps needed
Single machine with the same <i>TIBCO_HOME</i>	<ol style="list-style-type: none"> <li>1. TIBCO Service Performance Manager</li> <li>2. TIBCO Enterprise Message Service</li> </ol>	<p>Set <i>EMS_HOME</i> to the TIBCO Enterprise Message Service installation directory in the following files.</p> <p>For the SPM server:</p> <ul style="list-style-type: none"> <li>• <i>TIBCO_HOME</i>/spm/2.3/bin/setems4spm.bat</li> <li>• <i>TIBCO_HOME</i>/spm/2.3/bin/tibspm.tra</li> <li>• <i>TIBCO_HOME</i>/spm/2.3/bin/tibspmddlgenerator.tra</li> <li>• <i>TIBCO_HOME</i>/spm/2.3/bin/tibspmexamples.tra</li> <li>• <i>TIBCO_HOME</i>/spm/2.3/bin/tibspmpassword.tra</li> </ul>
Single machine with different <i>TIBCO_HOME</i>	Any order	<p>For the SPM dashboard:</p> <ul style="list-style-type: none"> <li>• <i>TIBCO_HOME</i>/amxdashboard/3.4/amxdashboard/startspmdashboard.bat</li> <li>• <i>TIBCO_HOME</i>/amxdashboard/3.4/amxdashboard/tomcat/bin/setenv.bat</li> <li>• <i>TIBCO_HOME</i>/amxdashboard/3.4/amxdashboard/tomcat/bin/service.bat</li> <li>• <i>TIBCO_HOME</i>/amxdashboard/3.4/setup/install.properties</li> </ul>

Setup Details	Installation Order	Steps
Different machines where TIBCO Enterprise Message Service is installed on machine 1 and TIBCO Service Performance Manager on machine 2		<ul style="list-style-type: none"> <li>Perform the following steps:               <ol style="list-style-type: none"> <li>Copy the following files from TIBCO_HOME/spm/2.3/bin of machine 2 to EMS_HOME/lib of machine 1: setems4spm.bat and setems4spm.scr</li> <li>Execute setems4spm.bat.</li> </ol> </li> <li>Ensure that the folder structure for EMS client libraries on local machine points to EMS_HOME/lib.</li> <li>Copy the folder structure EMS_HOME/lib from machine 1 to machine 2 and place it at the same level as TIBCO_HOME/spm/2.3.</li> <li>Verify the following files are present under EMS_HOME/lib on machine 2: jms.jar, tibjms.jar, slf4j*.jar, tibcrypt.jar               <div data-bbox="884 884 924 926" style="display: inline-block; vertical-align: middle;"></div> <div data-bbox="995 863 1437 957" style="border-left: 1px solid #0070c0; padding-left: 10px; margin-left: 10px;">                 You must replace jms.jar with jms-2.0.jar if you plan to use EMS v8.0+.               </div> </li> <li>Update all TRA and bat files to set EMS_HOME = TIBCO_HOME/spm/2.3</li> <li>Set the EMS_HOME in the following files. For the SPM server:               <ul style="list-style-type: none"> <li>TIBCO_HOME/spm/2.3/bin/setems4spm.bat</li> <li>TIBCO_HOME/spm/2.3/bin/tibspm.tra</li> <li>TIBCO_HOME/spm/2.3/bin/tibspmddlgenerator.tra</li> <li>TIBCO_HOME/spm/2.3/bin/tibspmexamples.tra</li> <li>TIBCO_HOME/spm/2.3/bin/tibspmpassword.tra</li> </ul>               For the SPM dashboard:               <ul style="list-style-type: none"> <li>TIBCO_HOME/amxdashboard/3.4/amxdashboard/startspmdashboard.bat</li> <li>TIBCO_HOME/amxdashboard/3.4/amxdashboard/tomcat/bin/setenv.bat</li> <li>TIBCO_HOME/amxdashboard/3.4/amxdashboard/tomcat/bin/service.bat</li> <li>TIBCO_HOME/amxdashboard/3.4/setup/install.properties</li> </ul> </li> </ul>



## Creating EMS Queues and Factories

The EMS Queues and factories are the channels provided by the EMS server to enable communication between the client and server.



The non-admin users need Send, Receive, and Browse permissions to access TIBCO Enterprise Message Service queues.

### Procedure

1. Go to `TIBCO_HOME/spm/2.3/bin` directory.
2. Make sure that correct `EMS_HOME` is set in all TRA and configuration files.
3. Open the `setems4spm.scr` file for editing.



If the EMS server and the Service Performance Manager server are on different machines, perform the following steps:

Open the `setems4spm.bat` file, and set `EMS_HOME=<EMS_HOME location of the local machine>`.

4. If the EMS server and the Service Performance Manager server are set up on different machines, edit `SPM_HOME/bin/setspm4ems.scr` script file and replace "localhost" with the appropriate IP address of the machine on which the TIBCO EMS server is running. For example:

instead of

```
connect tcp://localhost:7222
create factory SPMQueueConnectionFactory queue
url=tcp://localhost:7222
```

use

```
connect tcp://123.456.789.111:7222
create factory SPMQueueConnectionFactory queue
url=tcp://123.456.789.111:7222
```

5. Replace `//localhost` with IP address of the machine on which TIBCO Enterprise Message Service is running in all the property files and startup scripts.

For example,

```
connect tcp://10.97.122.174:7222
create factory SPMQueueConnectionFactory queue url=tcp://10.97.122.174:7222
```

6. Execute the following command to create the required queues and connection factories to be used by the server and client.

```
TIBCO_HOME/spm/2.3/bin/setems4spm.bat
```

7. Verify that the following queues are created in EMS:

```
>>created queue 'spm.inbound.query.queue'
>>created queue 'spm.ft.queue': exclusive
>>created queue 'spm.outbound.queue'
>>created queue 'spm.inbound.queue'
```

8. If you want to change the names of the connection factories and queues, make corresponding changes to the Service Performance Manager server, TIBCO ActiveMatrix Dashboard, and sample files.

## Setting Properties for the SPM Dashboard

To ensure that the dashboard works, you need to set some properties in the *TIBCO\_HOME/spm/2.3/spmdashboard/tomcat/bin/setenv.bat* file.

### Procedure

1. Open *TIBCO\_HOME/spm/2.3/spmdashboard/tomcat/bin/setenv.bat*.
2. Modify the property, *CATALINA\_OPTS* to have the correct remote host name, port number, SSL and authentication options, if any. The property is commented by default. The default setting of the property is as follows:

Platform	Command
<b>Windows</b>	<pre>set CATALINA_OPTS= -Dcom.sun.management.jmxremote - Dcom.sun.management.jmxremote.host=localhost -Dcom.sun.management.jmxremote.port=9600 - Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false</pre>
<b>Linux</b>	<pre>export CATALINA_OPTS= -Dcom.sun.management.jmxremote - Dcom.sun.management.jmxremote.host=localhost -Dcom.sun.management.jmxremote.port=9600 - Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false</pre>

3. Save the file.

## Configuring the SPM Dashboard Server to use the SPM Server

1. Stop TIBCO ActiveMatrix SPM server 2.3.1.
2. Copy all the files from *<SPM\_OLD\_TIBCO\_HOME>\spm\2.3\config* to *<SPM\_NEW\_TIBCO\_HOME>\spm\2.3\config*.
3. Copy the *.jar* file of the JDBC driver (for example, *postgresql-9.4-1202.jdbc4.jar*) from *<SPM\_OLD\_TIBCO\_HOME>\spm\2.3\lib\ext* to *<SPM\_NEW\_TIBCO\_HOME>\spm\2.3\lib\ext*. For the Oracle database, copy the *.jar* file from the folder which you used to configure the third-party driver while creating *CONFIG\_HOME* to *<SPM\_NEW\_TIBCO\_HOME>\spm\2.3\lib\ext*.
4. Set *EMS\_HOME* to the TIBCO Enterprise Message Service installation directory in the following files:

*TIBCO\_HOME/spm/2.3/bin/setems4spm.bat*

*TIBCO\_HOME/spm/2.3/bin/tibspm.tra*

*TIBCO\_HOME/spm/2.3/bin/tibspmdlgenerator.tra*

*TIBCO\_HOME/spm/2.3/bin/tibspmexamples.tra*

*TIBCO\_HOME/spm/2.3/bin/tibspmpassword.tra*

5. Copy *amx-rtruntime.jar* from *TIBCO\_HOME\amxspmdashboard\3.4\lib* to *TIBCO\_HOME\spm\2.3\lib*. (Replace the file if it already exists.)
6. Start TIBCO ActiveMatrix SPM server 2.3.1. For more information on starting the server, refer to [Starting the Server](#).

## Configuring TIBCO Service Performance Manager Dashboard Server

Use the TIBCO Configuration Tool to configure the following properties of the TIBCO ActiveMatrix Service Performance Manager (SPM) Dashboard.

- Generate Database Configuration
- Database Configuration
- JMS Configuration
- Threadpool Configuration
- Server Configuration
- Storage And Recovery Configuration
- Action Configuration
- Handle Configuration File
- Client API JMS Configuration
- Client API Configuration
- Dashboard Server Configuration
- Dashboard Server Security Configuration
- Dashboard Server Authentication LDAP Configuration
- Tomcat Server Configuration
- Dashboard Server Authentication File Configuration

For more information on these properties using TIBCO Configuration Tool, refer to [Configure TIBCO Service Performance Manager Dashboard](#).

## Configuring the TIBCO Service Performance Manager Server

Use the TIBCO Configuration Tool to configure the following properties of the Service Performance Manager server:

- Database configuration
- JMS configuration
- Threadpool configuration
- Server configuration
- Storage and recovery configuration
- Action configuration
- Handle Configuration File

For more information on these properties using TIBCO Configuration Tool, refer to [Configure TIBCO Service Performance Manager](#).

When the TIBCO Configuration Tool starts, initial data is loaded from `TIBCO_HOME/tct/components/shared/1.0.0/plugins/com.tibco.tct.spm_1.1.0.00X`. Alternatively, you can manually change the properties specified in the `TIBCO_HOME/spm/2.3/config/spm-config.properties` file.

### Procedure

1. Open the `spm-config.properties` file in the `SPM_HOME/config` folder for editing.
2. Uncomment the required property, and specify a new value.

## Result



TIBCO Configuration Tool does not recognize the changes made directly to the `spm-config.properties` file. Hence it is recommended to always use TIBCO Configuration Tool to make changes to the configuration.

## Generating the Database Schema and Starting the Database

You can either use the TIBCO Configuration Tool or use the `SPM_HOME/bin/tibspmdlgenerator` utility to generate the database schema.

### Procedure

1. Copy `AMX_3_0_SPM_Schema` from `TIBCO_HOME/amxspmdashboard/3.4/config` to `TIBCO_HOME/spm/2.3/config`. Select a `CONFIG_HOME` that is different from the one you used while configuring TIBCO Configuration Tool and create a new database user.
2. Generate the database schema:
  - a) Launch TIBCO Configuration Tool from `TIBCO_HOME/tct/1.6/TIBCOConfigurationTool` and select the **Configure TIBCO Service Performance Manager - V2.3**.
  - b) Select **Configure TIBCO Service Performance Manager Server**, provide the database credentials, and select the **Store Facts** check box in the **Storage and Recovery Configuration** screen.
  - c) Select **Generate TIBCO Service Performance Manager Database Schema**. Provide the **Config Folder**, **Output Folder**, and **Property File** locations. Click **Generate scripts**, click **Next**, and then click **Configure**.

The following files are generated in the database folder (for example: `TIBCO_HOME/spm/2.3/bin/oracle`):

```
spm_<database_type_name>_cleanupddl.sql
spm_<database_type_name>_createddl.sql
spm_<database_type_name>_dropddl.sql
```

3. Execute the DDL scripts generated in the previous step.



Ensure that the JDBC driver jar files compatible with the selected database is available to the server. To do so, add them in the `tibspm` classpath by either placing them in `TIBCO_HOME/spm/2.3/lib/ext` or by directly modifying the classpath in the chosen TRA file.

4. Create tables in database (Oracle, DB2, MySQL) using the `spm_oracle_createddl.sql` file.
  1. Connect to the database with the user details specified while configuring SPM in the **Configure TIBCO Service Performance Manager Server** screen of the TIBCO Configuration Tool.
  2. Copy content from file `spm_oracle_createddl.sql`, paste it into the database executable part, and execute it.

## Configuring TIBCO Service Performance Manager Service Probe

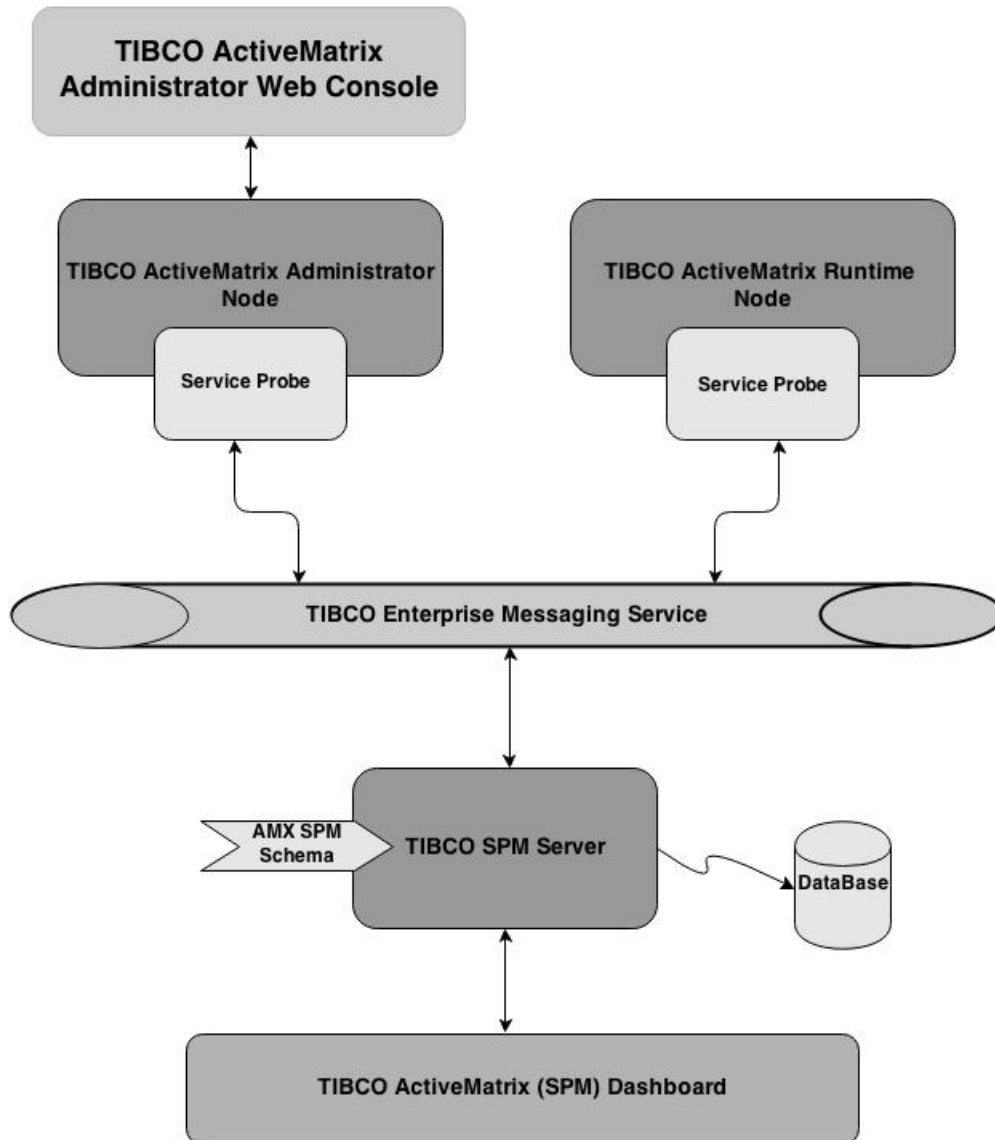
The service probe publishes service statistics and life-cycle events to TIBCO Service Performance Manager.

The TIBCO ActiveMatrix Administrator node publishes information about life-cycle events of TIBCO ActiveMatrix assets such as nodes, applications, services, and certain shared resource instance types to TIBCO Service Performance Manager. Additionally, it also publishes the availability details of the TIBCO ActiveMatrix assets on an hourly basis.

All TIBCO ActiveMatrix runtime nodes, where the service probe has been enabled, publish statistical information to the TIBCO Service Performance Manager over a TIBCO Enterprise Messaging Server queue. The following information is published:

- Service and Reference statistics
- Node JVM statistics
- Resource instance statistics for HTTP Connectors, JDBC, JMS Connection Factory and ThreadPool Shared Resources
- Metrics-related data to SPM for applications that use Virtualization Bindings, JMS Bindings, and SOAP Bindings

#### *Service Probe Architecture*



After the service probe is enabled on any TIBCO ActiveMatrix node, statistics are emitted periodically to the TIBCO Service Performance Manager server asynchronously via EMS. Additionally, the TIBCO ActiveMatrix Administrator node also emits asset status.

The TIBCO Service Performance Manager server receives the statistics from all the TIBCO ActiveMatrix nodes that have the service probe enabled. The TIBCO Service Performance Manager server then applies some statistical computations on the received data in real-time, stores it, and renders it via the TIBCO ActiveMatrix Dashboard, a presentation UI that is separate from TIBCO ActiveMatrix Administrator.

## Service Probe Installation Prerequisites

Before enabling the TIBCO ActiveMatrix installation with the service probe, install the following:

- TIBCO ActiveMatrix Service Grid
- TIBCO ActiveMatrix SPM Runtime Server

This section describes how to enable the service probe for your ActiveMatrix installation.

## Enabling the Service Probe on TIBCO ActiveMatrix Nodes

You can enable the TIBCO ActiveMatrix service probe from TIBCO ActiveMatrix Administrator UI or CLI.

Enabling the service probe on the SystemNode (that serves the TIBCO ActiveMatrix Administration application) is mandatory when TIBCO Service Performance Manager is being used. Additionally, the service probe should be enabled on the runtime nodes that need to be monitored.

While enabling the service probe on the runtime nodes is optional, it is recommended that the service probe be enabled on all nodes in an environment that needs to be monitored.



You must enable the probe on each newly created node. Make changes in `TIBCO_HOME/administrator/3.4/samples/spm/spm_probe_data`.

The TIBCO ActiveMatrix service probe publishes asset state to synchronize with TIBCO Service Performance Manager in the following two ways:



1. Periodically - on the hour.
2. Manually - when user refreshes Application(s) from TIBCO ActiveMatrix

TIBCO Service Performance Manager dashboard will not display the correct state for the applications unless one of the above two events take place. For example, when you restart a runtime node the state will not be updated until the periodic synchronization happens or you explicitly refresh the TIBCO ActiveMatrix Administrator.

## Enabling the Service Probe Using TIBCO ActiveMatrix Administrator UI



If TIBCO ActiveMatrix Administrator is replicated (or running in a replicated setup), enable the TIBCO Service Performance Manager probe on all replicated Administrator instances.

When you start a new administration setup using TIBCO Service Performance Manager, ensure that the TIBCO Service Performance Manager, server database is cleaned up. The TIBCO Service Performance Manager displays data on the dashboard by querying the database. If old data is retained in the database, then it gets displayed on the dashboard.

### Procedure

1. Login to TIBCO ActiveMatrix Administrator.
2. Click **Infrastructure>Nodes**. The Node details are displayed.
3. Select a node and from the bottom pane, click **Configuration**.
4. Click **JVM Configuration**.
5. Add the `spm.probe` and set its value to on.
6. Use the same steps to configure other TIBCO Service Performance Manager [client properties](#).

7. Click **Save** and then **Install** or **Sync** to synchronize node configuration.
8. Restart the node using the TIBCO ActiveMatrix Administrator to reflect the changes.

## Enabling the Service Probe Using TIBCO ActiveMatrix Administrator CLI

TIBCO ActiveMatrix Administrator Command-Line Interface (CLI) can help configure or update node JVM properties. You can use Administrator CLI scripts to enable Service Probe and to set TIBCO Service Performance Manager Client properties on TIBCO ActiveMatrix nodes.

Samples scripts can be found in `CONFIG_HOME\admin\<enterprise name>\samples\spm`.

For more information on Administrator Command-Line interface, refer to the section "Command-Line Interface" in the *TIBCO ActiveMatrix Service Grid Administration Guide*.

If TIBCO ActiveMatrix administrator is replicated (or running in a replicated setup), enable the TIBCO Service Performance Manager probe on all replicated Administrator instances.

### Procedure

1. Provide the TIBCO\_HOME location in the `TIBCO_HOME/administrator/<version>/samples/admin-scripts-base` file.
2. Add the `remote.properties` from `TIBCO_HOME/CONFIG_HOME/admin/amxadmin/samples/` to `TIBCO_HOME/administrator/<version>/samples/`.
3. Check EMS location in `spm_probe.properties` file.
4. On nodes you want to enable the probe, open `CONFIG_HOME\admin\<enterprise name>\samples\spm\spm_probe.properties` and set the following:  

```
set spm_probe=on
```
5. Go to `CONFIG_HOME\admin\<enterprise name>\samples\spm\spm_probe_data.xml`. Update the Environment, Node, and Host names.
6. Ensure that the correct information is specified in the `spm_probe.properties` file.

Ensure that the values of the following properties match the values specified on TIBCO Service Performance Manager:



- `spm_client_jms_jndi_url`
- `spm_client_connection_username`
- `spm_client_connection_password`
- `spm_client_jms_jndi_contextfactory`
- `spm_client_schema_name`

7. Ensure that the node is running before you execute these steps:
  - a) From `TIBCO_HOME/administrator/<version>/samples/spm`, run the following command:

```
ant -f spm_probe_build.xml
```

- b) Restart the affected nodes.



- To enable a service probe on a node, you must disable monitoring services.
- To receive timely updates from the TIBCO Service Performance Manager server, ensure that the service probe is enabled.

## Disabling the Service Probe on TIBCO ActiveMatrix Nodes

You can disable TIBCO ActiveMatrix service probe from TIBCO ActiveMatrix Administrator GUI or CLI.

You must start by disabling the service probe on all TIBCO ActiveMatrix Administrator nodes (including the replicated nodes) followed by the TIBCO ActiveMatrix runtime nodes.

### Disabling the Service Probe Using TIBCO ActiveMatrix Administrator UI

#### Procedure

1. Login to TIBCO ActiveMatrix Administrator.
2. Click **Infrastructure>Nodes**. The Node details are displayed.
3. Select a node and from the bottom pane, click **Configuration**.
4. Click **JVM Configuration**.
5. Add the property:  
Property: `spm.probe`  
Value: `off`
6. Click **Save** and then **Install** or **Sync** to synchronize the node configuration.
7. Restart the node using the TIBCO ActiveMatrix Administrator to reflect the changes.

### Disabling the Service Probe Using TIBCO ActiveMatrix Administrator CLI

#### Procedure

1. On nodes you want to disable the probe, open `<CONFIG_HOME>\admin\<enterprise name>\samples\spm\spm_probe.properties` and set the following:  

```
set spm_probe=off
```
2. Go to `<CONFIG_HOME>\admin\<enterprise name>\samples\spm\spm_probe_data.xml`. Update the Environment, Node, and Host names.
3. Ensure that the node is running before you execute these steps:
  1. Run `ant -f spm_probe_build.xml`.
  2. Restart the affected nodes.

### Client Properties of TIBCO Service Performance Manager



Property	Mandatory?	Default Value	Description
<code>spm.probe</code>	Yes	<code>off</code>	Property to enable or disable a service probe on TIBCO ActiveMatrix nodes.
<code>spm.client.connection.username</code>	Yes	<code>admin</code>	Specifies username of metric engine.





Property	Mandatory?	Default Value	Description
<code>spm.client.connection.password</code>	Yes		Specifies password for metric engine. This is obfuscated using the obfuscation utility shipped with the product.
<code>spm.client.jms.jndi.url</code>	Yes	<code>tibjmsnaming://localhost:7222</code>	Specifies JMS JNDI URL.
<code>spm.client.amx.schema.name</code>	No	<code>AMX_3_0</code>	The value of the name attribute of the Schema file. This Schema file is given as an input to TIBCO Service Performance Manager.
<code>spm.client.jvm.stat.interval.minutes</code>	No	<code>1</code>	Interval in minutes that a service uses to publish the JVM information of a node to TIBCO Service Performance Manager.
<code>spm.client.jms.jndi.contextfactory</code>	No	<code>com.tibco.tibjms.naming.TibjmsInitialContextFactory</code>	Specifies context factory class for the JMS provider.
<code>spm.client.jms.queueconnectionfactory</code>	No	<code>SPMQueueConnectionFactory</code>	Queue connection factory name. Needs to be pre-created.
<code>spm.client.abound.queue</code>	No	<code>spm.inbound.queue</code>	Queue name on JMS to perform sync/async operations.
<code>spm.client.jms.inbound.query.queue</code>	No	<code>spm.inbound.query.queue</code>	Queue name on JMS to perform snapshot query operations.
<code>spm.client.jms.outbound.queue</code>	No	<code>spm.outbound.queue</code>	Queue name on JMS for client to receive notifications from metric engine.
<code>spm.client.taskmgr.threadpool.size</code>	No	<code>5</code>	Number of threads to be used for fact publishing per session.
<code>spm.client.taskmgr.threadpool.keepalive.time</code>	No	<code>60</code>	Specifies the time (in seconds) to keep alive the task manager threads. When this time elapses, idle threads time out.
<code>spm.client.fact.queue.depth</code>	No	<code>1000</code>	Defines the queue depth for the internal queue for creating a batch of facts.

Property	Mandatory?	Default Value	Description
<code>spm.client.fact.batch.size</code>	No	1	Number of facts to batch before publishing to the TIBCO Service Performance Manager server. For TIBCO ActiveMatrix Administrator nodes which publishes lifecycle events, this value can be one. Having the value as one ensures that such events are published immediately. For TIBCO ActiveMatrix non-Administrator nodes the value can be different, say 100.
<code>spm.client.facts.retry.count</code>	No	INT_MAX	Maximum retries for a synchronous operation if it fails as a result of EMS disconnect.
<code>spm.client.fact.eviction.enabled</code>	No	true	Enable or disable asynchronous eviction of facts once the queue depth is full.  When disabled, eviction is done by thread putting the fact. Disabling it may result in more facts being lost if the fact batch size is high and the put rate is more than the consumption rate.
<code>spm.client.fact.eviction.frequency</code>	No	100	You can set this property only if <code>spm.client.fact.eviction.enabled</code> is set to true.
<code>spm.client.fact.batch.expiry</code>	No	5	Defines the amount of time in seconds to wait to flush residual facts if the batch size condition is not met.
<code>spm.client.heartbeat.interval</code>	No	60 * 1000	Specifies time interval in milliseconds used by named client sessions to send heartbeat.
<code>spm.client.sync.operation.retry.count</code>	No	3	Maximum retries for an operation in case it fails.
<code>spm.client.retry.count</code>	No	INT_MAX	Maximum retries for establishing connection to a transport provider.
<code>spm.client.retry.wait</code>	No	1000	Time in milliseconds to wait before retrying the operation.

Property	Mandatory?	Default Value	Description
<code>spm.client.sync.response.timeout</code>	No	10000	Time in milliseconds to wait for the TIBCO Service Performance Manager to wait for the server to send a response for a sync operation like query registration.
<code>spm.client.sync.jms.msg.expiry</code>	No	$5 * 60000 = 30000$	Time in milliseconds for the JMS provider to keep a message before it expires.
<code>spm.client.session.init.timeout</code>	No	LONG_MAX	Time to wait for the client session to complete.
<code>spm.client.session.init.timeout.timeunit</code>	No	TimeUnit.DAYS	The time unit for the wait for the <code>spm.client.session.init.timeout</code> property.
<code>spm.amx.events.queue.depth</code>	No	1000	Defines the queue depth for the internal TIBCO ActiveMatrix queue for creating a batch of TIBCO Service Performance Manager events.
<code>spm.amx.events.thread.pool.size</code>	No	Number of processes +1.	Defines the minimum number of threads to be used for publishing TIBCO ActiveMatrix events to the TIBCO Service Performance Manager fact queue.
<code>spm.amx.resource.stat.interval.minutes</code>	No	1 minute	<p>The TIBCO ActiveMatrix node publishes statistical information of a Shared Resource instance over the interval specified in this property.</p> <p>For shared resources, the fact emission interval is one minute. For an application service hit, it is real time.</p>

Property	Mandatory?	Default Value	Description
<code>spm.amx.app.name.filter</code>	No	<p>amx.artifactserver.ap, amx.logservice.app, amx.payloadservice.app, amx.dashboard-app, amx.platform-app, amx.governance.mcr.aggregator, com.tibco.amx.it, com.tibco.amx.bt, com.tibco.amx.platform, com.tibco.amx.mcr.aggregator, com.tibco.amx.commonlogging, GovernanceControlDistribution</p> <p> To filter additional application names, keeping the default intact, use the following format:</p> <p><code>spm.amx.app.name.filter = default,&lt;APPLICATION_NAME&gt;</code></p>	<p>List of comma-separated application names for which life cycle and statistical information is not sent to TIBCO Service Performance Manager.</p> <p> All application names which exactly match or start with the specified names are filtered.</p>

Property	Mandatory?	Default Value	Description
spm.amx.resource.name.filter	No	tibco.admin.http.connector.internal, amxAdminDefaultHttpConnector, tibco.admin.appdb.jdbc   To filter additional resource names, keeping the default intact, use the following format:  spm.amx.resource.name.filter = default,<USER_SPECIFIED_RESOURCE_NAME>	List of comma-separated resource names for which life cycle and statistical information is not sent to TIBCO Service Performance Manager.   All application names which exactly match or start with the specified names are filtered.

## Changing the Heap Size of the Server

You can change the heap size of the Service Performance Manager server.

### In the TRA File

You can change the heap size by specifying the properties in the corresponding TRA file, the default being tibspm.tra.

### In the Console Mode

You can set the initial and maximum heap size in the Console mode. Follow these steps if you start the server in console mode.

### Procedure

1. Open tibspm.tra.
2. Change the following properties:

```
java.heap.size.initial=128M
java.heap.size.max=256M
```



Do not explicitly add -Xms, -Xmx properties under java.extended.properties.

3. At the command prompt, uninstall the Windows NT service of the Service Performance Manager server using the following command:

```
tibspm -uninstall
```

4. At the command prompt, install the Service Performance Manager server using the following command:

```
tibspm -install
```

- Restart the service.



To run Service Performance Manager as a Windows NT service, ensure that the following properties in `spm-config.properties` are set with the absolute paths:

```
rta.schema.store=<TIBCO_HOME>/spm/<version>/config
```

## Logging Configuration

Each of the Service Performance Manager components uses log4j for application logging.

By default:

- Server logs are generated under `SPM_HOME/logs/spm.log`.
- TIBCO SPM Dashboard logs are generated under `SPM_HOME/logs/spmdashboard.log`.
- Example logs are generated under `SPM_HOME/logs/spmdemo.log`.

## SPM Server Logging Configuration

TIBCO Service Performance Manager server logs are at `SPM_HOME/logs/spm.log`.

### Application Log File Appender

```
log4j.appender.ApplicationRFileAppender=org.apache.log4j.RollingFileAppender
log4j.appender.ApplicationRFileAppender.File=SPM_HOME/logs/spm.log
log4j.appender.ApplicationRFileAppender.MaxFileSize=10MB
log4j.appender.ApplicationRFileAppender.MaxBackupIndex=10
log4j.appender.ApplicationRFileAppender.layout=org.apache.log4j.PatternLayout
log4j.appender.ApplicationRFileAppender.layout.ConversionPattern= %d{dd MMM yyyy}
HH:mm:ss,SSS zzz Z} %p %t [%c] - %m%n
```

The following appender in the `log4j.properties` file is used to log actions:

- Log Action File Appender

### Log Action File Appender

```
log4j.appender.LogActionAppender=org.apache.log4j.RollingFileAppender
log4j.appender.LogActionAppender.File=SPM_HOME/actionlogs/logaction.log
log4j.appender.LogActionAppender.MaxFileSize=10MB
log4j.appender.LogActionAppender.MaxBackupIndex=5
log4j.appender.LogActionAppender.layout=org.apache.log4j.PatternLayout
log4j.category.LogActionLogger=INFO, LogActionAppender
```

## SPM Dashboard Logging Configuration

The SPM dashboard logs are generated at `TIBCO_HOME/spm/2.3/logs/spmdashboard.log`.

You can configure these logs using the `TIBCO_HOME/spm/2.3/config/spm_dashboard_log4j.properties` log configuration file. Configure the log file path with the following property:

```
log4j.appender.dashboardAppender.File=./logs/spmdashboard.log
```



By default, Tomcat server logs are generated at `TIBCO_HOME/spm/2.3/spmdashboard/tomcat/logs`.

## SPM Example Logging Configuration

The example logs are generated at `TIBCO_HOME/spm/2.3/logs/spmdemo.log`.

You can configure these logs using the `TIBCO_HOME/spm/2.3/config/Demo_log4j.properties` log configuration file. Configure the log file path with the following property:

```
log4j.appender.RFileApp.File=TIBCO_HOME/spm/2.3/logs/SpmDemo.log.
```

# Using the Service Performance Manager Components

To use Service Performance Manager, you must configure the server, dashboard, and generate the database schema. After completing the configuration, you can start the server and the dashboard.

## Starting the TIBCO SPM Server

Before using the product for monitoring the services deployed, ensure that you start the server.

Start `tibspm` from `TIBCO_HOME/spm/2.3/bin`. By default, the `tibspm` uses `tibspm.tra` as its configuration file. If a different TRA file is being used, open the command prompt and use the following command:

```
tibspm --propFile <path to the .TRA file>
```

The server uses a configuration file as specified in the `application_args` property of the TRA file that is configured either using TIBCO Configuration Tool or manually.



Changes to any of the properties require a server restart.

## Starting the TIBCO SPM Dashboard

During installation, TIBCO Universal Installer renames the default `service.bat` (supplied by Apache Tomcat) in `SPM_HOME/spmdashboard/tomcat/bin` folder to `service-preSPM.bat`, and copies a new version of `service.bat`.

### Procedure

1. Edit `SPM_HOME/spmdashboard/tomcat/bin/service.bat` to substitute `%TIBCO_EMS_HOME_ESC%` with appropriate local TIBCO Enterprise Message Service installation path.



After you substitute, you can use this `service.bat` to start Apache Tomcat hosting the Service Performance Manager Dashboard application as a Windows Service using `service.bat {install | uninstall}` on a Windows command prompt. If you install it as a Windows Service, an entry - TIBCO SPM Dashboard appears in the services list (`services.msc`).

2. To use Enterprise Message Service 8.0.0 or later, edit the file `SPM_HOME/spmdashboard/tomcat/bin/setenv.bat` (or `setenv.sh`) and `service.bat` and change `"%EMS_HOME%/lib/jms.jar` to `%EMS_HOME%/lib/jms-2.0.jar`.



If you are working with a version earlier than 8.0, skip to the next step.

3. Start the TIBCO SPM Dashboard using one of the following methods:

- Click **Start > All Programs > TIBCO > SPM\_HOME > TIBCO Service Performance Manager <version> > Start SPM Generic Dashboard**.
- Go to the `SPM_HOME/spmdashboard` folder and run the following executables:  
`startspmdashboard.bat`

The UI for SPM Dashboard is available using Admin agent.

## Samples

There are a few examples that are bundled with the product. The samples can be located at *SPM\_HOME/examples*.

### Running the Client API Application Example

You can run the `tibspmxamples` to take a look at how the Client API application works.

#### Procedure

1. Open a command prompt and go to *TIBCO\_HOME/spm/2.3/bin*.
2. Stop the server. You can manually stop the server by clicking CTRL+C on the server window.
3. Restart the server by starting `tibspm` from *TIBCO\_HOME/spm/2.3/bin*. By default, the `tibspm` uses `tibspm.tra` as its configuration file.
4. Execute `tibspmxamples`.



Refer to the example source code distributed in `src.zip` to know how to use client Java API. You need to set appropriate `PATH` and `CLASSPATH` to compile and execute such programs. See `tibspmxamples.tra` to understand the list of all libraries needed.

The list of properties for configuring the samples that are shipped with the product are provided in [Client Properties](#).

### Client Properties

The client properties are used by the sample client program shipped with the product. The ActiveMatrix probe for TIBCO Service Performance Manager exposes a set of API properties that may be different from the set of client properties.

The client properties are only documented for sake of demonstrating the client API configuration capabilities.



- The client API does not recognize these properties. The client API only recognizes `ConfigProperty` elements.

The `Demo_config.properties` file includes a subset of the following client properties.

#### Client Properties

Property	Mandatory	Default Value	Description
<code>rta.client.connection.username</code>	Yes		Specifies username of metric engine.
<code>rta.client.connection.password</code>	Yes		Specifies password for metric engine.
<code>rta.client.jms.jndi.contextfactory</code>	No	<code>com.tibco.tibjms.naming.TibjmsInitialContextFactory</code>	Specifies context factory class for the JMS provider



Property	Mandatory	Default Value	Description
<code>rta.client.jms.jndi.url</code>	No	<code>tibjmsnaming://localhost:7222</code>	Specifies JMS JNDI URL
<code>rta.client.jms.queueconnectionfactory</code>	No	<code>SPMQueueConnectionFactory</code>	Queue connection factory name. Needs to be pre-created
<code>rta.client.jms.inbound.queue</code>	No	<code>spm.inbound.queue</code>	Queue name on JMS to perform sync/async operations
<code>rta.client.jms.outbound.queue</code>	No	<code>spm.outbound.queue</code>	Queue name on JMS for client to receive notifications from metric engine
<code>rta.client.taskmgr.threadpool.size</code>	No	5	Number of threads to be used for fact publishing per session
<code>rta.client.taskmgr.threadpool.keepalive.time</code>	No	60	Specifies the time (in seconds) to keep alive the task manager threads. When this time elapses, idle threads time out.
<code>rta.client.fact.queue.depth</code>	No	100	Defines the queue depth for the internal queue for batching facts
<code>rta.client.fact.batch.size</code>	No	1	Number of facts to batch before publishing to the server
<code>rta.client.fact.eviction.enabled</code>	No	true	Enable or disable async eviction of facts once the queue depth is full.  When disabled, eviction is done by thread putting the fact. Disabling it may result in more facts being lost if the fact batch size is high and the put rate is more than the consumption rate.
<code>rta.client.fact.eviction.frequency</code>	No	100	You can set this property only if <code>rta.client.fact.eviction.enabled</code> is set to true.
<code>rta.client.fact.batch.expiry</code>	No	5	Defines the amount of time in seconds to wait to flush residual facts if the batch size condition is not met.
<code>rta.client.heartbeat.interval</code>	No	60 * 1000	Specifies time interval in milliseconds used by named client sessions to send heartbeat

Property	Mandatory	Default Value	Description
rta.client.ping.interval	No	1000	Time interval in milliseconds used for ping with the server.
rta.client.retry.count	No	3	Maximum retries for an operation in case it fails
rta.client.retry.wait	No	1000	Time in milliseconds to wait before retrying the operation
rta.client.sync.response.timeout	No	10000	Time in milliseconds to wait for the rta engine to wait for the server to send a response for a sync operation like query registration
rta.client.sync.jms.msg.expiry	No	5 * 60000 = 300000	Time in milliseconds for the JMS provider to keep a message before it expires
rta.client.logmanager.class	No	"com.tibco.rta.log.impl.DefaultLogManager"	Specifies external log manager impl. * @see com.tibco.rta.log.LogManager * @see com.tibco.rta.log.LogManagerFactory
rta.client.async.dispatcher.max.pool.size	No	2147483647	The thread pool used for dispatching results from outbound queue to clients. For instance, streaming queries/commands.
rta.client.async.dispatcher.timeout	No	300000	The thread pool used for dispatching results from outbound queue to clients has an idle timeout in milliseconds.

## Overriding the Default Property Values

If required, you can override the default values of the client properties.

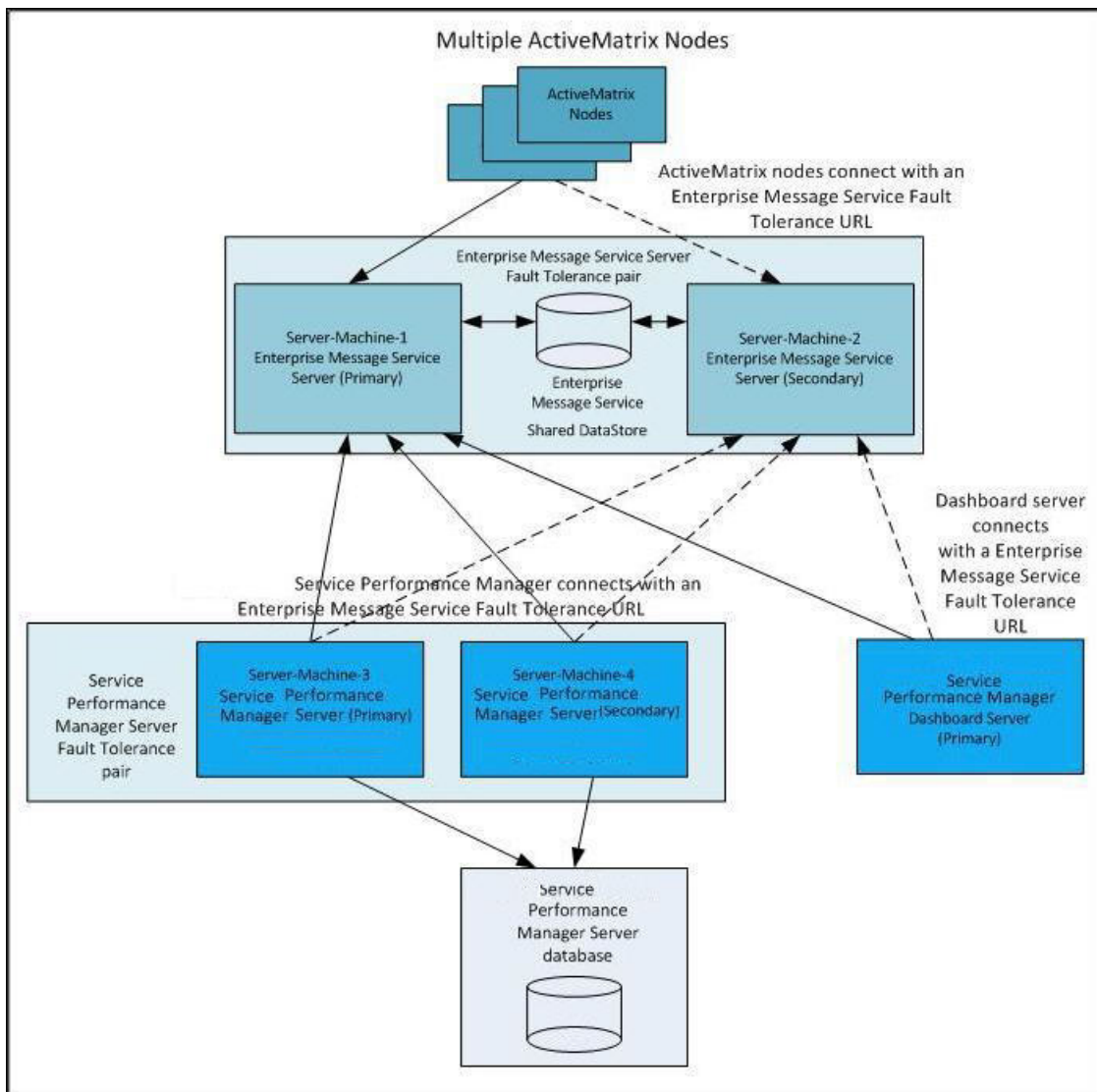
### Procedure

1. Open the `Demo-config.properties` file in the `SPM_HOME/config` folder for editing.
2. Uncomment the required property and specify a new value.

## Deployment Scenarios

Various deployment scenarios are supported by TIBCO Service Performance Manager.

The following diagram shows a recommended deployment of Service Performance Manager for TIBCO ActiveMatrix environment. It is however, not a product requirement. You can deploy one or more components on the same machine provided it has sufficient server resources.



You may not be able to achieve the required level of fault-tolerance if it is not deployed as per the recommendations.

## TIBCO Enterprise Message Service Server Deployment

TIBCO Service Performance Manager uses the Fault Tolerance feature of Enterprise Message Service.

Each of the primary and secondary Enterprise Message Service servers should be deployed on separate server machines to account for the Enterprise Message Service server machine level failures. They should share a common datastore. For more information on fault tolerance, refer to *TIBCO Enterprise Message Service User's Guide*.

## TIBCO Service Performance Manager Server Deployment

Each of the Service Performance Manager servers should also be deployed on separate server machines to account for the Service Performance Manager machine level failures.

You may start multiple instances of the Service Performance Manager server process on the same machine to account for the level failures of the Service Performance Manager server process on the same machine.

To connect to a fault tolerance enabled Enterprise Message Service pair, each of the Service Performance Manager server instances should use an Enterprise Message Service fault tolerance URL similar to the following:

```
rta.jms.jndi.url=tibjmsnaming://server-machine-1:7222, tibjmsnaming://server-machine-2:7222
```

TIBCO Service Performance Manager server uses the EMS Exclusive Queue feature for fault-tolerance. The server inbound queue over which the server receives messages should be configured as an exclusive queue. This is already done in the Enterprise Message Service setup script that is bundled with the product. Using an exclusive queue ensures that the Enterprise Message Service server always delivers messages only to the first connection on that queue. Hence, only one Service Performance Manager server is primary at any time. When this primary instance fails, Enterprise Message Service automatically starts to deliver the messages to any one of the remaining connections in that queue.

## Improving the Performance

There are several factors that contribute towards the performance of TIBCO Service Performance Manager.

The following are the recommendations for performance improvement.

### Client Batching

TIBCO Service Performance Manager Client API supports a time and count based batch. Whenever a time threshold or a count threshold is reached, the batch of facts is bundled as a single message and sent to the EMS server. The optimization is because the database inserts a batch of facts in a single transaction and all associated metric computations for this batch as a single database transaction per hierarchy.

### Server Batching

In addition to client batching, server side batching is also performed. Client batches are further batched inside the server for processing, for enhanced performance.

### Do not save facts, if possible

If you do not save facts, you get the best performance. If facts need to be saved, determine how many of them can be stored, since it would impact performance.

### Size the facts table and purge frequencies

If you choose to save the facts, it is very important to keep the size of the facts table in check such that performance is not impacted.

### Do not use processed facts table

Maintenance of yet another set of tables increases the load on the database to a great extent. Rely on TIBCO Enterprise Message Service for failures and recovery processing.

### Use a large L1 cache

We recommend using as much RAM as possible and a proportionately large L1 cache.

### Use a machine with large number of cores

Each of the dimension hierarchies as defined in the schema, takes up one CPU core for processing. Besides, a large number of threads would be required to efficiently serve streaming queries, snapshot queries, and rule evaluations. We recommend a multicore server class machine for running the Service Performance Manager server.

## Use an optimized Oracle setup

Database must be optimized for enhanced performance.

## Data Retention Policies

By default, data (facts) in TIBCO Service Performance Manager is persisted to a database. Unless deleted, the FACT table in the database grows with time. TIBCO Service Performance Manager enables you to purge the older data from the system. Facts are deleted based on the `created_time` of the fact.

### Retention Policy for FACTS

The older data can be purged periodically from the system using the following settings defined in the schema XML file:

```
<schema name="AMX_3_0" display-name="ActiveMatrix Service Grid 3.x">
  <retention-policies>
    <retention-policy type="fact" period="1" unit="DAY" purge-time-of-day="-1" purge-
    frequency-period="3600000"/>
  </retention-policies>
</schema>
```

Where:

- `type`: Set the value of this attribute to "fact" to configure a retention policy for facts.
- `period`: A number, to be used along with the attribute "unit". These two attributes together define how much data is to be retained.  
  
For example, setting `period=1` and `unit="DAY"`: If you set `period=1` and `unit="DAY"`, all facts older than one day are purged. If you set `period=2` and `unit="WEEK"`, all facts older than two weeks are purged. Possible values for unit are "DAY", "WEEK", and "HOUR".
- `purge-time-of-day`: Specify the time of the day when the purge activity would be scheduled. It takes the format HHMM where HH is the hour of the day and MM is the minute of the hour. For example, setting it to 0100 would schedule the first purge activity for 01 AM. Use -1 if you want the purge activity to be repeated every `purge-frequency-period`.
- `purge-frequency-period`: Specify how often to run the purge activity. Specify the time period in milliseconds.

### Retention Policy for Metrics and Hierarchies

Use a retention policy in the schema XML to configure the retention policy for dimension hierarchies. For metric hierarchy tables, metrics are purged based on `updated_time` of the metric. The value of the `type` attribute should be a fully-qualified name of a dimension hierarchy as defined in the schema. All other attributes have the same meaning as defined in the previous section. For example, the first line in the following example, prompts TIBCO Service Performance Manager to purge all metrics data that is older than 2 weeks, for the hierarchy `DevNodeCube/SrvTrends`. It is configured to run at 01 AM and with a frequency of 1 day (86400000 milliseconds).

```
<retention-policy type="DevNodeCube/SrvTrends" period="2" unit="WEEK" purge-time-of-
day="0100" purge-frequency-period="86400000"/>
```

Similarly, you can configure the retention policy of all other hierarchies by modifying the schema file.

The defaults for TIBCO Service Performance Manager are as shown in the following table:

#### *Level, Dimension, and Measurement based on Hierarchy*

Retention Policy Time	Period	Unit	Purge Time of Day	Purge Frequency Period
fact	1	DAY	-1	3600000

Retention Policy Time	Period	Unit	Purge Time of Day	Purge Frequency Period
DevNodeCube/SrvTrends	2	WEEK	0100	86400000
DevNodeCube/ApplTrends	2	WEEK	0110	86400000
DevNodeCube/NodeTrends	2	WEEK	0120	86400000
DevNodeCube/By Service	2	WEEK	0130	86400000
DevNodeCube/SvcInstTrends	2	WEEK	0140	86400000
DevNodeCube/GrpByClientIPRes	2	WEEK	0150	86400000
DevNodeCube/GrpBySrvClientIP	2	WEEK	0200	86400000
DevNodeCube/HttpResource	2	WEEK	0210	86400000
DevNodeCube/JdbcResource	2	WEEK	0220	86400000
InfCube/InferredStatus	2	WEEK	0230	86400000
Assets/env	2	WEEK	0240	86400000
Assets/app	2	WEEK	250	86400000
Assets/node	2	WEEK	300	86400000
Assets/node_hist	2	WEEK	0310	86400000
Assets/svcinst	2	WEEK	0320	86400000
Assets/svcinst_hist	2	WEEK	0330	86400000
Assets/http	2	WEEK	0340	86400000
Assets/http_hist	2	WEEK	0350	86400000
Assets/jdbc	2	WEEK	0400	86400000
Assets/jdbc_hist	2	WEEK	0410	86400000



Data can be deleted by the database administrator directly. If this is the preferred option, the administrator can set the values in the schema file to very large values such that the purge times are effectively disabled.

# Using TIBCO Business Studio

TIBCO Business Studio is packaged with TIBCO ActiveMatrix and can be installed through the **Studio Development Profile** during installation. Refer to the [Installation](#) section for more details on installing TIBCO Business Studio.



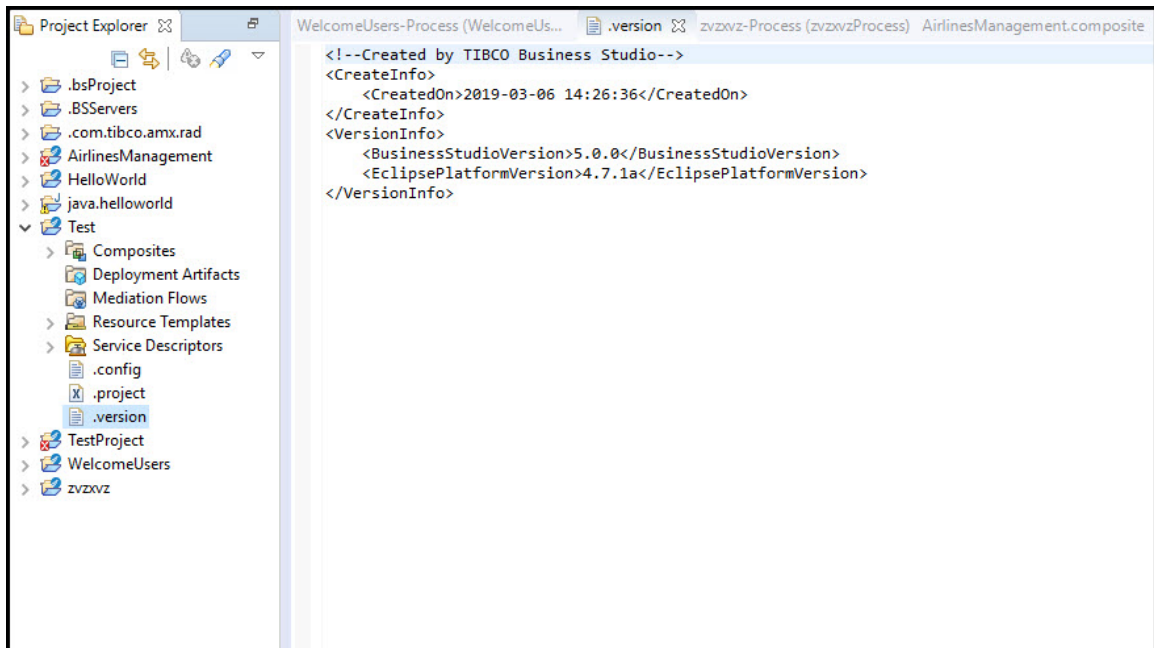
Do not install a new TIBCO Business Studio on an existing TIBCO\_HOME (with an older version of TIBCO Business Studio). Install TIBCO Business Studio in a separate TIBCO\_HOME.

TIBCO Business Studio is located in the TIBCO\_HOME/studio/<version> folder after the installation. The previous version of TIBCO Business Studio is located in the TIBCO\_HOME/studio/3.x folder.

Business Studio also supports Java<sup>TM</sup> 8 including language enhancements, search and refactoring, quick assist and clean up to migrate anonymous classes to lambda expressions and back, and new formatter options for lambdas. Existing Java projects created using an earlier version of Business Studio can be imported into Business Studio and then modified to use the Java 8 features, to be subsequently compiled using Java 8. The Deployment Archive Artifacts (DAAs) of Composites containing Java Implementation Type (IT) components implemented in Java 8 are backward compatible with TIBCO ActiveMatrix 3.3.0 (Hotfix 009 and higher) and can be deployed successfully in environments with JRE<sup>TM</sup> 8 Runtime support.

Additionally, TIBCO ActiveMatrix Binding Type for REST support is included by default in Business Studio, that is, no additional configuration is required to add and configure REST Service and Reference Bindings.

To identify TIBCO SOA projects that have been created or modified using this version of Studio, a hidden .version file is added to the TIBCO SOA and implementation project folders. This file contains important information about the project, such as timestamp, Studio version and Eclipse Platform version of creation or modification.



For more information on the .version file, refer to the "Finding out the Version of TIBCO Business Studio Using which a Project was Created" section of the *Composite Development Guide*.

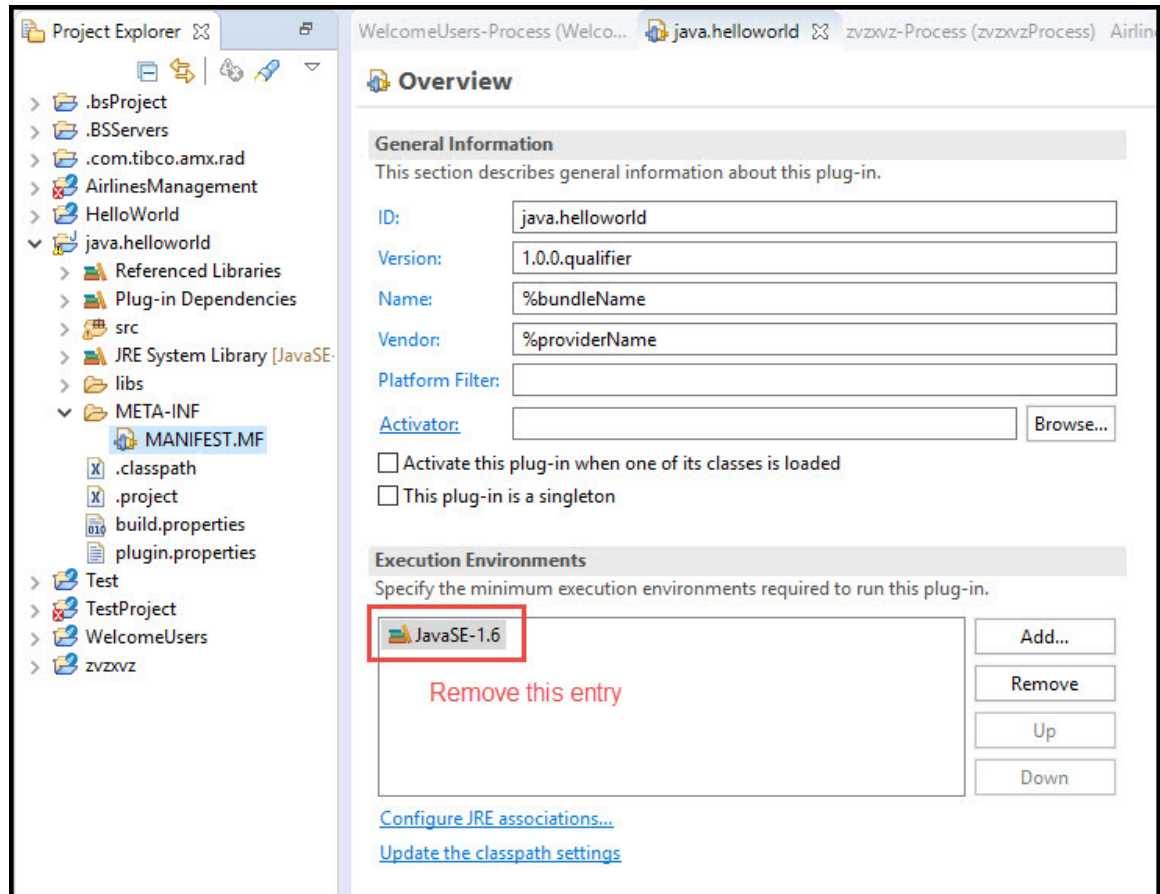
## Importing an Existing Java Project

To import a project created using an earlier version of TIBCO Business Studio:

1. Import the existing SOA project in the workspace.



2. Open the `MANIFEST.MF` file of the Java implementation project, located under `/META-INF/`.
3. In the **Overview** tab, remove the entry from **Execution Environments**, if present as shown below:



4. Clean the project using **Projects > Clean**.
  - Clean projects selected below option
  - Clean all projects option

The JRE System Library now uses JavaSE-1.8.
5. Add code using Java 8 features and proceed with the TIBCO SOA project design and DAA creation per usual.

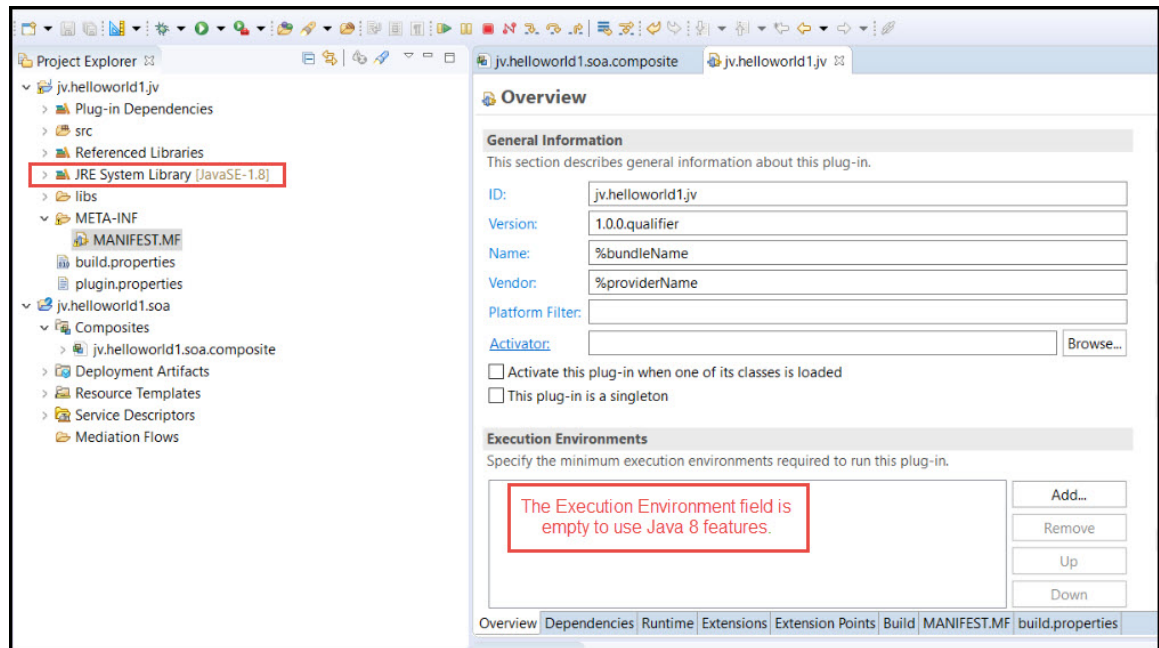


For information on known issues related to removing Execution Environments, refer to the Known Issues section of the *Release Notes*.

### Creating a New Java Project Using TIBCO Business Studio

1. Select **File > New > Project > TIBCO SOA Platform > TIBCO SOA Project**.
2. Add a Java implementation type component.
3. Select the Java implementation type component, right-click and select **Generate Java Implementation**.
4. Open the `MANIFEST.MF` file of the Java Implementation project located under `/META-INF/`.





It uses JavaSE-1.8 as JRE System Library.

5. Add code using the Java 8 features and proceed with the TIBCO SOA project design and DAA creation as usual.



You can refer to the sample available in `TIBCO_HOME\amx\<version>\samples\java\helloworld5.zip`. This sample introduces you to the Java 8 features.



On Mac, when code for a Java Implementation Type is generated, one of the following errors is listed in the **Problems** tab:

- **Syntax error, annotations are only available if source level is 1.5 or greater**
- **Syntax error, parameterized types are only available if source level is 1.5 or greater**

To fix this, you must upgrade the Java compiler to 1.8. To do this:

1. In the **Problems** tab, right-click and select **Quick Fix**.
2. In the **Quick Fix** dialog, select **Upgrade Java Compiler to 1.8**.
3. Click **Finish**.

# Upgrade and Downgrade

Upgrading the TIBCO ActiveMatrix environment entails installing a new release of TIBCO ActiveMatrix and upgrading the configuration of the different runtime objects such as hosts, ActiveMatrix Administrator servers, and nodes. Optionally, it may involve upgrading Enterprise Message Service (EMS) used by the ActiveMatrix Administrator servers and hosts.

You can upgrade to the current release of ActiveMatrix Service Grid using the TIBCO Configuration Tool (TCT) available in `TIBCO_HOME\tct\`.

If you plan to have a replicated configuration, do so before upgrading to the current release of ActiveMatrix Service Grid.



In a production environment, you can set up your system to include a replicated Administrator server on a second machine. Requests can be processed by either server. If one server is unavailable, the other server can process requests. For more details on a replicated configuration, refer to the [Replicate TIBCO ActiveMatrix Administrator Server](#) section.

The upgrade or downgrade process is robust, simple, and seamless. It consists of the following main steps:

1. Stop hosts before proceeding with the upgrade or downgrade.
  2. Upgrade or downgrade runtime hosts and nodes.
  3. Perform post-upgrade actions (only for an upgrade).
  4. Update runtime object information in ActiveMatrix Administrator.
  5. Restart hosts after a successful upgrade or downgrade.
- When upgrading, ActiveMatrix Administrator host or SystemHost must be upgraded *first*. That is, before upgrading any runtime host and node.
  - When downgrading, ActiveMatrix Administrator host or SystemHost must be downgraded *last*. That is, after downgrading all runtime hosts and nodes.
  - It is a good practice to have ActiveMatrix Administrator in the Running state while upgrading or downgrading runtime hosts and nodes.
  - If you have hosts that are running as Windows Services and you intend to start them after upgrading or downgrading them, you must start the TIBCO Configuration Tool (TCT) wizard with Administrator privileges.
  - Upgrade is idempotent. That is, if you try to upgrade a host which is already upgraded, it does not affect the host. Also, if you face any issues during upgrade, you can re-run upgrade after resolving the issues.



## Prerequisites for Upgrading or Downgrading

Before proceeding with upgrading or downgrading your enterprise, ensure that you perform the following steps:

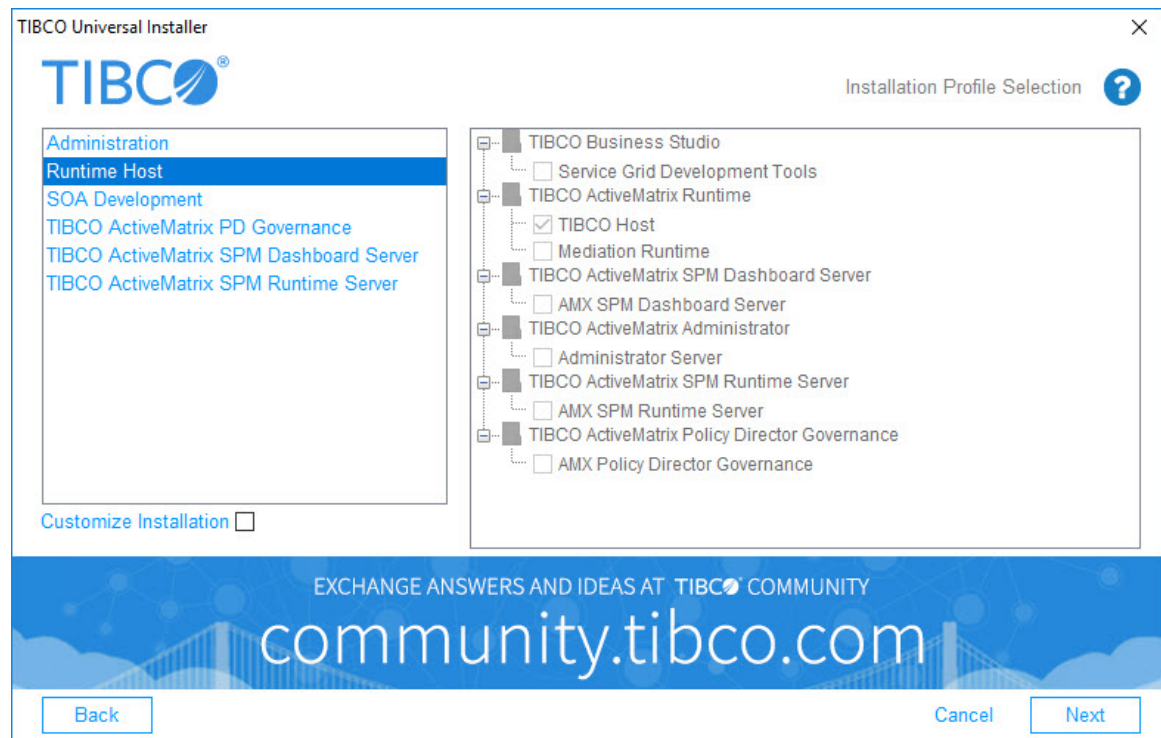
- Backup the `CONFIG_HOME` folder of your enterprise.  
In case of a failure, the TCT wizard reverts the changes made to runtime automatically. However, it is recommended that you take a backup.
- Backup the database instance that is configured with ActiveMatrix Administrator.
- Backup the database used by the Payload and Logging service, if they are not using the same database as the ActiveMatrix Administrator database.

- Make sure the minimum hard disk space is available. For example, the total disk space required is approximately 200MB for each host in the CONFIG\_HOME and an additional 300MB for the entire CONFIG\_HOME.
- If you plan to upgrade multiple hosts at the same time, increase the maximum memory in the TIBCOConfigurationTool.ini file that is located at TIBCO\_HOME\tct\. If the CONFIG\_HOME has more than 30 hosts and you are planning to upgrade all of them together in one TCT session, increase the maximum memory.
- Stop all hosts and nodes that are being upgraded or downgraded.
- Install ActiveMatrix 3.4.0 on the same TIBCO\_HOME where the earlier version was installed.



The Installation Profile should be selected depending on the profiles that are already existing in the TIBCO\_HOME. If the current TIBCO\_HOME contains ActiveMatrix Administrator or Business Studio or Runtime Host profiles, select and install the respective installation profile or combination of them using the Universal Installer.

- Install the **Runtime Host** profile **Mediation Runtime** Feature, if a Node managed by the Runtime Host contains an Application that is running Mediation. To install the **Runtime Host** profile **Mediation Runtime** Feature, during installation, select the **Customize Installation** check box, select the **Runtime Host** profile, and select **Mediation Runtime** as shown in the following screen. This is because ActiveMatrix Administrator automatically provisions the Mediation Product Feature to the Runtime Host while installing the application on the Node even though the Mediation feature was not installed on that TIBCO\_HOME.



- In the above scenario, when the runtime host is upgraded without installing the Mediation Feature, upgrade fails with the following error (sample from the TCT console log):

```
[patchmgr.Upgrade] Exception : product feature
com.tibco.amx.it.mediation.product.feature: 3.6.0 not found in any local machine
model
```

In this case, install the Runtime Profile again on the TIBCO\_HOME along with the Mediation feature. After installing, upgrade the Runtime Host again.

- To upgrade TIBCO ActiveMatrix Policy Director Governance, select the **TIBCO ActiveMatrix PD Governance** installation profile while installing ActiveMatrix Service Grid 3.4.0. TIBCO

ActiveMatrix Policy Director Governance is upgraded automatically as a part of ActiveMatrix Service Grid 3.4.0 upgrade.

- Run the diagnostic tests from the TCT Wizard to make sure the pre-requisites are met.

## Upgrade

Before you start the upgrade process, make sure you understand the impact the upgrade will have on your environment, and how various ActiveMatrix versions can coexist.

Upgrading your ActiveMatrix enterprise means upgrading the configuration of certain services and runtime objects. TIBCO provides a TIBCO Configuration Tool (TCT) wizard that you run to perform the upgrade process. The TCT wizard also allows you to run preliminary diagnostic tests and provides options to select runtime hosts in the enterprise that you want to upgrade.

To upgrade without difficulty, knowledge of the supported scenarios, upgrade impact, and the various steps in the upgrade process is helpful, and is summarized in the following sub-sections.

### Supported Upgrade and Downgrade Scenarios

Following table lists the eligibility of various versions of ActiveMatrix platform for upgrading to ActiveMatrix 3.4.0 or downgrading from ActiveMatrix 3.4.0.

Version	Eligible for Upgrading to ActiveMatrix 3.4.0?	Can be Downgraded from ActiveMatrix 3.4.0?
ActiveMatrix 3.3.1 or ActiveMatrix 3.3.1 (with Hotfixes)	Yes	Yes
ActiveMatrix 3.3.0 (with Hotfixes) upgraded to ActiveMatrix 3.3.1 (with Hotfixes)	Yes	ActiveMatrix 3.4.0 can only be downgraded to ActiveMatrix 3.3.1 (with Hotfixes)
ActiveMatrix 3.2.0 (with Hotfixes) upgraded to ActiveMatrix 3.3.1 (with Hotfixes)	Yes	ActiveMatrix 3.4.0 can only be downgraded to ActiveMatrix 3.3.1 (with Hotfixes)
ActiveMatrix 3.3.0 upgraded to ActiveMatrix 3.3.1	Yes	ActiveMatrix 3.4.0 can only be downgraded to ActiveMatrix 3.3.1
ActiveMatrix 3.3.0 or ActiveMatrix 3.3.0 (with Hotfixes)	Yes	Yes
ActiveMatrix 3.2.0 upgraded to ActiveMatrix 3.3.0	Yes	ActiveMatrix 3.4.0 can only be downgraded to ActiveMatrix 3.3.0
ActiveMatrix 3.1.x upgraded to ActiveMatrix 3.3.0	Yes	ActiveMatrix 3.4.0 can only be downgraded to ActiveMatrix 3.3.0
ActiveMatrix 3.2.0 or ActiveMatrix 3.2.0 (with Hotfixes)	Yes	Yes
ActiveMatrix 3.1.x upgraded to ActiveMatrix 3.2.0	Yes	ActiveMatrix 3.4.0 can only be downgraded to ActiveMatrix 3.2.0

Version	Eligible for Upgrading to ActiveMatrix 3.4.0?	Can be Downgraded from ActiveMatrix 3.4.0?
ActiveMatrix 3.1.x	No	No

### Version Coexistence

In an enterprise, the hosts or nodes could have a version that is different from the ActiveMatrix Administrator that manages them. For example, in 3.4.0, ActiveMatrix Administrator can be upgraded to 3.4.0 while the host it manages could be running on an older version (3.3.0 or 3.2.0) and they can still coexist.



Some Administration-related features (for example: updating a host's JVM parameters, downloading log files, and so on) will not work on these hosts and nodes which are "not upgraded" .

When a runtime host is upgraded to 3.4.0, all the nodes managed by that host are also upgraded to 3.4.0. As a result, the host and the nodes it manages are in sync and run the same version of ActiveMatrix.

### Exceptions to Version Coexistence

As a rule, a Deployment Artifact Archive (DAA) can only be used with nodes whose version is greater than or equal to the Studio version used to create the DAA. For example, a DAA created by ActiveMatrix 3.3.0 requires nodes running ActiveMatrix 3.3.x or higher (for example, 3.4.0).

To find out the node version, you can use the `tibcohost.exe describeNodes` command or use the ActiveMatrix Administrator UI Nodes tab. An example of the `tibcohost` command is shown below:

```
>tibcohost.exe describeNodes
```

The output of the command is:

```
Invoking describeNodes
Description of node "DevNode" follows:
Node description: Development node
Current status: RUNNING
Node type: com.tibco.amf.hpa.tibcohost.node.hibernate.feature
Node type version: 3.4.0
Platform version: 3.4.0
Start mode: auto
...
...
```

The following scenarios are an exception to version coexistence:

DAA Created in Studio of	Can be used with	Cannot be used with
ActiveMatrix 3.4.0	ActiveMatrix 3.4.0 Nodes	ActiveMatrix 3.3.1 Nodes
For information on how you can find out the version of Business Studio, refer to the "Finding out the Version of TIBCO Business Studio Using which a Project was Created" section of the <i>Composite Development Guide</i> .		ActiveMatrix 3.3.0 Nodes
		ActiveMatrix 3.2.0 Nodes
		ActiveMatrix 3.1.5 Nodes

DAA Created in Studio of	Can be used with	Cannot be used with
ActiveMatrix 3.3.1	ActiveMatrix 3.3.1 (and higher) Nodes  ActiveMatrix 3.3.0 Nodes (provided Nodes are running with Java 1.8)	ActiveMatrix 3.2.0 Nodes  ActiveMatrix 3.1.5 Nodes
ActiveMatrix 3.3.0	ActiveMatrix 3.3.0 (and higher) Nodes	ActiveMatrix 3.2.0 nodes  ActiveMatrix 3.1.5 nodes
ActiveMatrix 3.2.0	ActiveMatrix 3.2.0 (and higher) Nodes	ActiveMatrix 3.1.5 nodes
ActiveMatrix 3.1.5	ActiveMatrix 3.1.5 (and higher) Nodes	Nodes that are on versions prior to ActiveMatrix 3.1.5.



While planning replication, ensure that both the Administrator Servers have the same set of software versions including the Hotfixes that were applied before upgrading to ActiveMatrix 3.4.0.



If your Application (DAA) deploys and runs fine in an earlier version of TIBCO ActiveMatrix 3.4.0 but does not work properly in TIBCO ActiveMatrix 3.4.0 environment, then check the logs to see if it is because of the Application's dependency on some Third Party Component Library (TPCL) jars whose TIBCO ActiveMatrix 3.4.0 version drops export of some packages. If yes, then manually add those imports in your projects, rebuild and regenerate DAA, and deploy again.

## Upgrading Runtime Hosts and Nodes

While upgrading a host, all nodes that are managed by that host are also upgraded. There is no separate workflow for upgrading nodes. The TCT upgrade/downgrade wizard only shows a list of hosts for you to select for upgrade.

Upgrading the host entails the following:

### 1. Installing product features on a host

New version of the product features are installed on the host. Before installing the product features the Host Manager gets the currently installed product features from the host and installs the new version for only those product features. Also, the product features that are completely new in ActiveMatrix 3.4.0 will be installed.

### 2. Enabling product features on a node

New product features that are installed on the host are enabled on all the nodes managed by that host. This will make sure that the runtime nodes now run with the latest software.

### 3. Disabling old product features

Old version of the product features are disabled from all the nodes managed by the host.



The old product features are not uninstalled from the host (that is, features are not removed from the CONFIG\_HOME).

### 4. Updating JRE version of all hosts and nodes to version 1.8.0.

This is done internally when the hosts and nodes are updated to use ActiveMatrix 3.4.0 `rpflauncher_classpath_3.4.0.tra` file.

### 5. REST BT system applications installed previously are removed from all the nodes, if found.

The dependency of all the REST BT user applications is updated to depend on platform application.



6. BPM system applications, `amx.bpm.app` and `amx.bpm.apacheds`, are stopped.
7. Updating executables of all hosts and node (for example, `tibcohost.exe`) to use new wrapper version 2.4.7.

This will change the icons of all the executables (in Windows).

8. Platform application of all the nodes are now upgraded to a new version.

All the above steps can be verified in the upgrade logs. A sample output of all the above steps is provided in the [Example: Upgrade Scenario](#) section.

## Post Upgrade Actions

The TIBCO Configuration Tool (TCT) Upgrade or Downgrade wizard uses the `updateManifest` command of the Host Manager internally to update the software dependencies to be compatible with the current release of ActiveMatrix Service Grid. This includes system application dashboard client component dependency and the `javax.servlet` package dependency.

In the post-update action, manifest files of the jars and plugins running in the host are updated to expand the `javax.servlet` package dependency range so that it works with Jetty. With this, the current version of the jars running in the host are compatible with ActiveMatrix 3.4.0 without user intervention.

This action updates all the features installed by ActiveMatrix platform, ActiveMatrix system applications, all web applications (both system and user) and the features/applications uploaded by the users.



To see what are the changes that the post install action will be doing, you can perform a dry run of the post install action before upgrading. This can be done using the `dryRun` option of the `updateManifest` command of the HostManager.

For example, run the following command:

```
>tibco_hostmgr.exe updateManifest -configHomeLocation <CONFIG_HOME> -instanceNames
<my-instance> -clearCache -dryRun
```

A sample output of the command is shown below:

```
Following is the list of all tibcohost instances in config_home E:\amxconfig\admin1
Admin-amxadmin-instanceOne
```

```
Updating the manifest for following instance : "Admin-amxadmin-instanceOne"
```

```
INFO: Updating the bundles in Node name: "DevNode"
```

```
The Manifest Updater searching in the directory : 'E:\amxconfig\admin1\tibcohost
\Admin-amxadmin-instanceOne\data_3.2.x\nodes\DevNode\work\cf'
```

```
INFO: Updating the bundles in Node name: "SystemNode"
```

```
The Manifest Updater searching in the directory : 'E:\amxconfig\admin1\tibcohost
\Admin-amxadmin-instanceOne\data_3.2.x\nodes\SystemNode\work\cf'
```

```
The Component Details
```

```
Application name : 'com.tibco.amx.platform.dashboard'
```

```
Component Name : 'DashBoardWebApp'
```

```
Component ID : '76d6dc95-3fc2-4a8f-a941-93f8cd15a16a'
```

```
Component Path : 'E:\amxconfig\admin1\tibcohost\Admin-amxadmin-instanceOne
\data_3.2.x\nodes\SystemNode\work\cf\76d6dc95-3fc2-4a8f-a941-93f8cd15a16a'
```

```
Before com.tibco.amx.dashboard.client version = [1.0.0,1.0.100)
```

```
After com.tibco.amx.dashboard.client version = [1.0.0,2.0.0)
```

```
INFO: Bundle file updated of location : 'E:\amxconfig\admin1\tibcohost\Admin-
amxadmin-instanceOne\data_3.2.x\nodes\SystemNode\work\cf\76d6dc95-3fc2-4a8f-
a941-93f8cd15a16a\bundle'
```

```
The Component Details
```

```
Application name : 'com.tibco.amx.platform.artifactserver'
```

```
Component Name : 'ArtifactServer'
```

```
Component ID : '911ff791-ea69-4de0-b939-fb41b7744c61'
```

```
Component Path : 'E:\amxconfig\admin1\tibcohost\Admin-amxadmin-instanceOne/
data_3.2.x\nodes\SystemNode\work\cf\911ff791-ea69-4de0-b939-fb41b7744c61'
```

```
Before javax.servlet.http version = [2.5.100,3.0.0)
After javax.servlet.http version = [2.5.100,4.0.0)
```

You can refer to the [Example: Upgrade Scenario](#) section for a sample output of the logs after updating the `javax.servlet` package dependency.

To skip the post install step, you can uncheck the **post install action** check box in the TCT Upgrade/Downgrade summary screen.

It is recommended to enable post-upgrade action on the Administrator instance. If you do not want to run the post-upgrade action, manually update the applications to depend on the new `javax.servlet` package and un-check post upgrade action while upgrading.



If the dependencies are not updated, node start fails with errors in the node logs.

In this case, update the application depending on `javax.servlet` package manually and re-deploy the application OR select the **post install action** checkbox and run the upgrade again.



If you have existing CLI scripts that were running with ActiveMatrix Service Grid 3.3.x setup and if you have upgraded to ActiveMatrix Service Grid 3.4.0, the existing `build.xml` CLI scripts must be updated to include `<import file="${TIBCO_HOME}/administrator/3.4/scripts/basic_cli.xml" />` instead of `<import file="${TIBCO_HOME}/administrator/3.3/scripts/basic_cli.xml" />`.

## Creating and Installing Resource Template, Resource Instance required for Service Health Check

If you have upgraded to ActiveMatrix Service Grid 3.4.0 from earlier version, you need to create resource template, resource instance and install resource instance required for running Service Health Check from Administrator UI. Run following commands to create resource template, resource instance and install resource instance which are required to run Service Health Check from Administrator UI.

### Procedure

1. Open a command window.
2. Go to the directory `CONFIG_HOME/admin/enterprise_name/samples`.



Ensure that the name of the Node in the `resourceinstanceforshc_data.xml` file (on which the resource template and resource instance need to be created and installed) is same as the Administrator Node (SystemNode or SystemNodeReplica) name.

3. Run the following command to create resource template required for running Service Health Check.  
`ant -f resourcetemplateforshc_build.xml`
4. Run `ant -f resourcetemplate_build.xml create`
5. Run the following command to create and install resource instance.  
`ant -f resourceinstanceforshc_build.xml`
6. Run `ant -f resourceinstance_build.xml create install`

## Updating ActiveMatrix Administrator

Updating ActiveMatrix Administrator does not involve any manual steps and is triggered automatically when the Administrator node or system node is started after the upgrade process is complete.

Also see [Upgrading REST Binding Type](#).

Upgrading ActiveMatrix Administrator involves:

1. ActiveMatrix Administrator needs to be upgraded first. When ActiveMatrix Administrator gets restarted after the upgrade, it updates itself as follows:



- a. Upgrading platform application to version 3.4.0.

To verify, select the platform application from the ActiveMatrix Administrator UI. In the **Description** field, the platform application description is updated to reflect the version.

```
Default platform application [Upgraded from ActiveMatrix 3.3.1 to
ActiveMatrix 3.4.0 on 06/14/2018]
```

- b. Upgrading artifact server Application to version 3.4.0.
  - c. Updating plugins that are enabled on Nodes to 3.4.0 features.
  - d. REST BT system applications are removed and all user applications using REST BT are updated to depend on the platform application.
2. A runtime host needs to be restarted to complete the upgrade. After the ActiveMatrix Administrator receives a notification from the runtime host, the ActiveMatrix Administrator updates the host version accordingly.
  3. A runtime node needs to be restarted to complete the upgrade. After the ActiveMatrix Administrator receives a notification from the runtime node, ActiveMatrix Administrator performs the following actions for the runtime node:
    - a. Updating node version accordingly.
    - b. Upgrading platform application to version 3.4.0. The platform application description is updated to reflect the version. Select the platform application from the ActiveMatrix Administrator UI and in the **Description** field you can see comments like:

For example:

```
Default platform application [Upgraded from ActiveMatrix 3.3.1 to
ActiveMatrix 3.4.0 on 06/14/2018]
```

- c. Updating plugins that are enabled on nodes to 3.4.0 features.
- d. REST BT system applications are removed and all user applications using REST BT are updated to depend on the platform application.



- If you upgrade the host but do not start them, ActiveMatrix Administrator will still show the old version for that host.
- If you have nodes in manual modes and they are not started after the upgrade, ActiveMatrix Administrator will still show the old version for that node (unless node is restarted after the upgrade).

## Upgrading REST Binding Type

REST BT is integrated with the ActiveMatrix Platform Application by default and is not required to be installed separately.

The upgrade process handles the add-on REST BT as follows:

1. The add-on REST BT product features are disabled and removed from all nodes and hosts before upgrade.
2. While upgrading the SystemNode or the Administrator node, REST BT Administrator Plugin is provisioned. This can be verified from the ActiveMatrix Administrator > Admin Configuration > Plug-ins UI screen after upgrading to 3.4.0.

## Plug-ins

Name	Version	Modified By	Modified On	State
TIBCO ActiveMatrix Administrator	3.4.0		2018-12-23 14:51:14	DEPLOYED
TIBCO ActiveMatrix Administrator Plug-in for Trinity Credential Server	3.4.0		2018-12-19 16:20:34	DEPLOYED
TIBCO Composite Application Platform Governance Common Administrator Plug-in	3.4.0		2018-12-19 16:20:34	DEPLOYED
TIBCO ActiveMatrix Administrator plugin for JMS Binding	3.4.0		2018-12-19 16:20:34	DEPLOYED
TIBCO ActiveMatrix JMS Resource Adapter Administrator Plugin	3.4.0		2018-12-19 16:20:34	DEPLOYED
TIBCO ActiveMatrix Administrator Plug-in for Common Logging	3.4.0		2018-12-19 16:20:35	DEPLOYED
TIBCO ActiveMatrix Metrics Collection Runtime Administrator Plug-in	3.4.0		2018-12-19 16:20:35	DEPLOYED
TIBCO ActiveMatrix Operations Governance Platform Administrator plug-in	3.4.0		2018-12-23 14:51:15	DEPLOYED
TIBCO ActiveMatrix Administrator Governance Policy Director admin plug-in	3.4.0		2018-12-23 14:51:13	DEPLOYED
TIBCO ActiveMatrix Policy Enforcement Runtime Administrator Plug-in	3.4.0		2018-12-19 16:20:35	DEPLOYED
TIBCO ActiveMatrix REST BT Administrator Plug-in	3.4.0		2018-12-23 14:51:13	DEPLOYED
TIBCO ActiveMatrix SOAP BT Administrator Plug-in	3.4.0		2018-12-19 16:20:35	DEPLOYED
TIBCO ActiveMatrix Administrator Plug-in for UDDI Server	3.4.0		2018-12-19 16:20:36	DEPLOYED

- The following REST BT system applications that are installed by the REST BT add-On are removed from all the nodes:

- `com.tibco.amx.bt.rest.Application.admin`
- `com.tibco.amx.bt.rest.Application`

The following screen shot shows that the above REST BT system applications that were available in 3.3.0 were removed after the upgrade.

Name	Application State	Last Deployed On	Synchronization	Action History
amx.platform.apps	Running	2017-02-20 14:42:47	In Sync	Deploy with Start Successful
com.tibco.amx.platform.artifactserver	Running	2017-02-20 14:42:59	In Sync	Deploy with Start Successful
com.tibco.amx.platform.dashboard	Running	2017-04-27 15:39:39	In Sync	Deploy with Start Successful

REST BT will be available when the platform application is upgraded. REST BT (binding.rest) is now available as a component in the `com.tibco.amx.platform` system application. This can be verified from the components list screen of the application.

Name	Application State	Last Deployed On	Synchronization	Action History
amx.platform.apps	Running	2018-12-19 16:19:59	In Sync	Start Successful
com.tibco.amx.platform (SystemNode)	Running	2018-12-19 16:25:55	In Sync	Deploy with Start Successful
com.tibco.ampd.ogp.de	Running	2018-12-19 16:26:20	In Sync	Deploy with Start Successful
com.tibco.ampd.psm	Running	2018-12-19 16:23:54	In Sync	Deploy with Start Successful
com.tibco.amx.commonlogging.logservice.app	Running	2018-12-19 16:24:28	In Sync	Deploy with Start Successful
com.tibco.amx.commonlogging.payloadservice.app	Running			

com.tibco.amx.platform (SystemNode)	
General	Configuration   Governance   Properties   Policy Set   UDDI Publication   Distribution   Substitution Variables   Resource Templates   Status
View	Currently Configured
com.tibco.amx.runtime.application	Details   Wires   Properties   Substitution Variables   Dependencies
GovernanceAgentPT	Description
ComponentFrameworkService	Component Type: Spring Component
GovernanceAgentListenerPT	Component Version: 1.0.0
ComponentFrameworkStatusN	Synchronization: In Sync
Implementation.java-spring	Start   Stop
Implementation.webapp	
binding.soap	
binding.rest	
messaging.bus.abstract.to.em	
messaging.bus.ems.to.abstrac	
messaging.bus	

Node Name	Component State	Component Action History
SystemNode	Running	Start successful

- All the user and system applications that are using REST BT will be automatically updated to depend on the platform application.
- ActiveMatrix Administrator, when started for the first time after upgrading SystemNode or Administrator node, automatically updates the database to reflect the changes made in the runtime. For example, REST BT system applications are removed from the database and all REST BT applications are updated to depend on the platform application.

## Upgrading TIBCO Service Performance Manager

Use the following steps to upgrade TIBCO Service Performance Manager:

1. Stop TIBCO ActiveMatrix SPM server 2.3.1.
2. Copy all the files from <SPM\_OLD\_TIBCO\_HOME>\spm\2.3\config to <SPM\_NEW\_TIBCO\_HOME>\spm\2.3\config.
3. Copy the .jar file of the JDBC driver (for example, postgresql-9.4-1202.jdbc4.jar) from <SPM\_OLD\_TIBCO\_HOME>\spm\2.3\lib\ext to <SPM\_NEW\_TIBCO\_HOME>\spm\2.3\lib\ext. For the Oracle database, copy the .jar file from the folder which you used to configure the third-party driver while creating CONFIG\_HOME to <SPM\_NEW\_TIBCO\_HOME>\spm\2.3\lib\ext.
4. Set EMS\_HOME to the TIBCO Enterprise Message Service installation directory in the following files:
 

```
TIBCO_HOME\spm\2.3\bin\setems4spm.bat
TIBCO_HOME\spm\2.3\bin\tibspm.tra
TIBCO_HOME\spm\2.3\bin\tibspmdlgenerator.tra
TIBCO_HOME\spm\2.3\bin\tibspmexamples.tra
TIBCO_HOME\spm\2.3\bin\tibspmpassword.tra
```
5. Copy amx-rtruntime.jar from TIBCO\_HOME\amxspmdashboard\3.4\lib to TIBCO\_HOME\spm\2.3\lib. (Replace the file if it already exists.)
6. Start TIBCO ActiveMatrix SPM server 2.3.1. For more information on starting the server, refer to [Starting the Server](#).

## Upgrading TIBCO ActiveMatrix Policy Director Governance

This section describes how to upgrade an existing installation of TIBCO ActiveMatrix Policy Director Governance.

If ActiveMatrix Policy Director Governance is already installed and configured with the previous version of ActiveMatrix Service Grid, upgrading to ActiveMatrix Service Grid 3.4.0 will automatically upgrade ActiveMatrix Policy Director Governance. You must select the **TIBCO ActiveMatrix PD Governance** installation profile while installing ActiveMatrix Service Grid 3.4.0. **TIBCO ActiveMatrix PD Governance** is available as a separate installation profile.

If ActiveMatrix Policy Director Governance is not installed and configured with the previous version of ActiveMatrix Service Grid, upgrading to ActiveMatrix Service Grid 3.4.0 will not upgrade ActiveMatrix Policy Director Governance (if ActiveMatrix Policy Director Governance is not installed through the installation profile).

If you want to enable and configure ActiveMatrix Policy Director Governance after upgrading to ActiveMatrix Service Grid 3.4.0, you can install ActiveMatrix Policy Director Governance in the same TIBCO\_HOME and use TCT wizard to configure ActiveMatrix Policy Director Governance with existing ActiveMatrix Administrator server.

## Supported ActiveMatrix Policy Director Governance Upgrade Scenarios

TIBCO ActiveMatrix Policy Director Governance that is installed in one of the following installation scenarios can be upgraded while upgrading to ActiveMatrix Service Grid 3.4.0:

From Version	Eligible for Upgrading to ActiveMatrix Service Grid 3.4.0?
Policy Director 1.0.0 or Policy Director 1.0.0 with Hotfixes	Yes
Policy Director 1.0.1 or Policy Director 1.0.1 with Hotfixes	Yes

From Version	Eligible for Upgrading to ActiveMatrix Service Grid 3.4.0?
Policy Director 1.0.0 upgraded to Policy Director 1.0.1	No
Policy Director 1.0.0 or 1.0.1 upgraded to Policy Director 1.1.0	No
Policy Director 1.1.0	Yes
Policy Director 1.1.0 with Policy Director 1.1.0 Hotfix 001 (upgraded to ActiveMatrix Service Grid 3.3.1)	Yes

### Upgrading TIBCO ActiveMatrix Policy Director Governance Installation in TIBCO ActiveMatrix Service Grid 3.3.x

This scenario assumes that you have TIBCO ActiveMatrix Service Grid 3.3.x installed and also have one of the version from TIBCO ActiveMatrix Policy Director version 1.1.0, 1.0.0 or 1.0.1 configured. You now need to upgrade to TIBCO ActiveMatrix Policy Director Governance which is integrated with ActiveMatrix Service Grid 3.4.0.

#### Procedure

1. Stop the TIBCO Host instance (**tibcohost**).
2. Install TIBCO ActiveMatrix Service Grid 3.4.0 in the same <TIBCO\_HOME> as previous version of TIBCO ActiveMatrix. Refer to the [Installation](#) section for details on how to do this. Select **TIBCO ActiveMatrix PD Governance** installation profile while installing ActiveMatrix Service Grid.
3. Follow the instructions in [Upgrade](#) section to upgrade TIBCO ActiveMatrix Service Grid to version 3.4.0.

ActiveMatrix Policy Director Governance will get upgraded automatically as part of ActiveMatrix Service Grid 3.4.0 upgrade.

### Upgrading TIBCO ActiveMatrix Policy Director Governance Installation on TIBCO ActiveMatrix Service Grid 3.2.x

This scenario assumes that you have TIBCO ActiveMatrix Service Grid 3.2.x installed and also have TIBCO ActiveMatrix Policy Director 1.0.0 or 1.0.1 configured. You now need to upgrade your TIBCO ActiveMatrix Policy Director Governance which is integrated with ActiveMatrix Service Grid 3.4.0.

#### Procedure

1. Stop TIBCO Host instance (**tibcohost**).
2. Install TIBCO ActiveMatrix Service Grid 3.4.0 in the same <TIBCO\_HOME> as previous version of TIBCO ActiveMatrix. Refer to the [Installation](#) section for details on how to do this. Select **TIBCO ActiveMatrix PD** installation profile while installing ActiveMatrix Service Grid.
3. Follow the instructions in [Upgrade](#) section to upgrade your TIBCO ActiveMatrix Service Grid to version 3.4.0.

ActiveMatrix Policy Director Governance will get upgraded automatically as part of ActiveMatrix Service Grid 3.4.0 upgrade.

## Verifying the Upgrade

1. Check the ActiveMatrix Administrator version in the ActiveMatrix Administrator UI > About link. It should contain "TIBCO ActiveMatrix® Administrator Version 3.4.0".
2. Check the application version for the platform app and the artifact server app.  
These applications should now be using the 3.4.0 version of the application template. Also, the description should indicate that the application has been upgraded or downgraded.
3. In the CONFIG\_HOME/tibcohost/<HOST\_NAME>/data\_3.2.x/host/th/version.properties file, make sure the value of the tibcohost.version property is 3.4.0.
4. Make sure the Administrator plugins version in ActiveMatrix Administrator is 3.4.0.
5. Check the version of hosts (**Infrastructure > Hosts**) and nodes (**Infrastructure > Nodes**) in the ActiveMatrix Administrator UI. The version must be 3.4.0.
6. The ActiveMatrix platform application should be updated to use the new application template version 3.4.0. For example, com.tibco.amx.platform Application.
7. TIBCO ActiveMatrix platform application (com.tibco.amx.platform) must be Healthy and in **Running** state.
8. From any host that has been upgraded, execute the following command from the CONFIG\_HOME\tibcohost\<HOST\_NAME>\host\bin folder to see the version history of the host or node. The last one should be the latest version and it should show 3.4.0.

```
>tibcohost.exe describeHost
>tibcohost.exe describeNodes
```

This command shows the upgrade history along with other properties of the host/node which confirms that ActiveMatrix 3.4.0 is installed and host/node has been upgraded successfully.



Even though the upgrade history of the describeHost command shows the associated patch(es) as amx.platform.patch:3.4.0, the actual software running in the hosts are not patched during upgrade. They are entirely new.

9. From the TIBCO\_HOME/amx/3.4/bin folder, execute the following command to show the version history of the specified Host. The last one should be the latest version and it should show 3.4.0.
10. After upgrading to ActiveMatrix 3.4.0, a new UI option **Enterprise Status** will be available under the **Infrastructure** menu.
11. All host and node executables will be updated and will display the new TIBCO Logo (only on Windows). Also, the --version command on the executable will show the new version as 2.4.7.

```
>tibamx_Hostmanager.exe describeHostUpgradeHistory
```

To verify the upgrade, refer this [checklist](#).

## Uninstalling MCR Dashboard Application

If you had the MCR Dashboard Application installed in your previous setup but are not using it, or not intending to use it in TIBCO ActiveMatrix Service Grid 3.4.0, it is recommended that you uninstall the MCR Dashboard Application using the following steps:

### Procedure

1. In ActiveMatrix Administrator UI, click **Applications**.
2. Select **SystemEnvironment** from the Environment drop-down list.
3. Expand the **System** folder.

4. Select `com.tibco.amx.platform.dashboard` from the Applications list and click **Undeploy**.
5. If the `com.tibco.amx.mcr.aggregator` Application is also in the Applications list, select the application and click **Undeploy**.
6. Restart the node.

## Downgrade

Downgrading the ActiveMatrix enterprise means downgrading the configuration of certain services and runtime objects. TIBCO provides TCT wizard that you run to perform the downgrade process. The TCT wizard also allow you to run preliminary diagnostic test and provides options to select runtime hosts of your enterprise that you want to downgrade.

### Prerequisites

New actions that are performed on the upgraded platform will potentially cause the downgrade to fail because of the compatibility issues. It is important to understand and proactively verify the state of the enterprise that will help to downgrade without any issues.

The following are some cases that could break the downgrade and the required actions to be taken before the downgrade.

- **Check for unbound hosts**

A new host that is created using the TIBCO Configuration Tool and is not bound or registered to ActiveMatrix Administrator cannot be downgraded. Do not select this unbound host for downgrade. Alternatively, remove the unbound hosts from the enterprise before downgrade.

If `CONFIG_HOME` has any host that is not bounded to ActiveMatrix Administrator (that is, the host is created using TCT, but not yet bounded to any ActiveMatrix Administrator), do not select such unbounded host for downgrade. Selecting such unbounded host fails the downgrade process.

- **Check for new nodes created in 3.4.0**

When a new node is created after upgrading platform to ActiveMatrix 3.4.0, it cannot be downgraded to previous version. A host that contains the new node cannot be downgraded because the node does not exist in the previous version. Remove these new nodes before the downgrade or do not select these hosts from the list of hosts in the TCT wizard before downgrade. It is recommended to remove these nodes because after downgrading ActiveMatrix Administrator there may be compatibility issues in an earlier version of ActiveMatrix Administrator managing 3.4.0 nodes.

If the user still downgrades the hosts that are created after upgrading to 3.4.0, they will be skipped and the upgrade procedure/scripts will not fail and will proceed to downgrade other hosts (if multiple hosts are selected).

- **Check for the HTTP Connector shared resource created after upgrading to ActiveMatrix 3.4.0**

HTTP Connector resource in ActiveMatrix 3.4.0 contains new properties that are not supported in the older version of ActiveMatrix (3.3.0 or earlier). As a result, after downgrade, these HTTP connector resource instances might go into a Not Running state and the applications using them might be in a Start Failed state. Refer to the [Troubleshooting](#) section to recover from this error state after the downgrade.



Before downgrading from ActiveMatrix Service Grid 3.4.0 to ActiveMatrix Service Grid 3.3.1, update TIBCO JRE to the JRE 8 Update 162 or lower using command line (`TIBCO_HOME\amx\<version>\bin\amx_jre_updater.exe`). For more information, see [TIBCO ActiveMatrix JRE Updater](#).





If you have upgraded from an earlier version of TIBCO ActiveMatrix (including hotfixes) to TIBCO ActiveMatrix 3.4.0 and if you have installed and applied TIBCO ActiveMatrix 3.4.0 hotfix, when you revert the TIBCO ActiveMatrix 3.4.0 hotfix, downgrading to the earlier version of TIBCO ActiveMatrix is not supported. The same is applicable to an earlier version of TIBCO ActiveMatrix setup configured with TIBCO ActiveMatrix Policy Director Governance.

## Downgrading Runtime Hosts and Nodes

While downgrading a host all the nodes that are managed by that host will also be downgraded. There is no separate workflow for downgrading nodes. TCT Upgrade or Downgrade wizard only shows a list of hosts that you can select for downgrade.

Following steps are performed while downgrading the host:

### 1. Installing product features on host

Old version of the product features are installed on the host. Before installing the product features the Host Manager gets the currently installed product features from the host and installs the old version for only those product features. Also the product features that are completely new in ActiveMatrix 3.4.0 for which the corresponding old version cannot be found are removed.

### 2. Enabling product features on node

Old product features that are installed on the host are enabled on all the nodes managed by that host. This makes sure that the runtime nodes now run with the preferred version of the software.

### 3. Disabling and uninstalling ActiveMatrix 3.4.0 product features

ActiveMatrix 3.4.0 version of the product features are disabled from all the nodes managed by the host and then they are uninstalled from the host.

### 4. Downgrading JRE version and Wrapper version

Hosts and nodes are updated to use JRE version that they were using before upgrading to 3.4.0. Similarly, all host and node executables are updated to use the wrapper version before downgrade.

### 5. Downgrading platform application of all the nodes to an old version

This is done by removing the ActiveMatrix 3.4.0 platform application and provisioning the old platform application (from the backup) directly in the runtime node.

## Updating ActiveMatrix Administrator

Updating ActiveMatrix Administrator does not involve any manual steps and is triggered automatically when the Administrator node or System Node is started after the downgrade process is complete.

Updating ActiveMatrix Administrator involves:

1. ActiveMatrix Administrator needs to be running and downgraded last. All other hosts and nodes need to be downgraded and restarted before downgrading ActiveMatrix Administrator.
2. A runtime host needs to be restarted to complete downgrade. After the ActiveMatrix Administrator receives a notification from the runtime host, ActiveMatrix Administrator updates the host version accordingly.
3. A runtime node needs to be restarted to complete downgrade. After the ActiveMatrix Administrator receives a notification from the runtime node, ActiveMatrix Administrator updates the following for the runtime node:
  - a. Node version
  - b. Downgrading platform application to the previous version.

To verify, select the platform application from the ActiveMatrix Administrator UI. In the **Description** field, the platform application description is updated to reflect the version.

Default platform application [Upgraded from ActiveMatrix 3.3.1 to ActiveMatrix 3.4.0 on 07/19/2018 23:05:38] [Downgraded from ActiveMatrix 3.4.0 to ActiveMatrix 3.3.1 on 07/19/2018 23:12:51]

- c. Updating plugins that are enabled on the node to features of the previous version
  - d. Adding REST BT system applications and marking applications as 'out of sync' if they use REST BT.
4. ActiveMatrix Administrator must be downgraded last. It updates itself as follows during downgrade:
- a. Downgrading platform application to the previous version.

To verify, select the platform application from the ActiveMatrix Administrator UI. In the **Description** field, the platform application description is updated to reflect the version.

Default platform application [Upgraded from ActiveMatrix 3.3.1 to ActiveMatrix 3.4.0 on 07/19/2017 23:05:53] [Downgraded from 3.4.0 to 3.3.1 on 07/19/2018 23:12:46]

- b. Downgrading artifact server application to the previous version.
- c. Updating plugins that are enabled on the node to features of the previous version.
- d. Adding REST BT system applications and marking applications as 'out of sync' if they use REST BT.

## Downgrading REST Binding Type

If there are applications deployed with REST BT, ActiveMatrix Administrator creates REST BT system applications automatically, and marks all applications with REST BT as out of sync. These REST BT system applications and applications with REST BT need to be deployed manually after downgrade.

When downgrading from 3.4.0 to 3.3.0 or lower, the ActiveMatrix downgrade process handles REST BT as follows:

1. REST BT product features are added back for all nodes and hosts.
2. The following REST BT system applications installed by the REST BT add-on are added for all the nodes:

`com.tibco.amx.bt.rest.Application.admin`

`com.tibco.amx.bt.rest.Application`

Name	Application State	Last Deployed On	Synchronization	Action History
System				
com.tibco.amx.bt.rest.application_3.3.0	Not Deployed		Out of Sync	
com.tibco.amx.bt.rest.application.admin_3.3.0	Not Deployed		Out of Sync	
rest-java_1	Partially running	2017-04-27 15:39:39	Out of Sync	Deploy with Start Successful

3. All the user and system applications that are using REST BT will be marked as out of sync.

Name	Application State	Last Deployed On	Synchronization	Action History
System				
com.tibco.amx.bt.rest.application_3.3.0	Not Deployed		Out of Sync	
com.tibco.amx.bt.rest.application.admin_3.3.0	Not Deployed		Out of Sync	
rest-java_1	Partially running	2017-04-27 15:39:39	Out of Sync	Deploy with Start Successful

These REST BT system applications and applications with REST BT must be deployed manually after downgrade as follows:



1. Start host and node if they are not running.
2. Deploy all REST BT system applications.
3. Stop host and node.
4. Uninstall ActiveMatrix 3.4.0 from the `TIBCO_HOME` where the ActiveMatrix Administrator Instance was running. For more details on uninstalling ActiveMatrix 3.4.0, refer to [Uninstalling TIBCO ActiveMatrix Service Grid in the GUI Mode](#) described in the [Upgrading and Downgrading: An Example](#).
5. Start ActiveMatrix Administrator host and node.

After all REST BT system applications are fully running, restart all runtime nodes which have applications with REST BT.

Now, all applications with REST BT are out of sync and in the `Waiting for dependencies` state.

6. Deploy these applications to bring them back to `Running`.

## Verifying the Downgrade

1. Check the ActiveMatrix Administrator version in the ActiveMatrix Administrator UI > About link. It should show the version where you upgraded ActiveMatrix Administrator from.
2. Check host and node version in ActiveMatrix Administrator UI, they must be prior to ActiveMatrix 3.4.0.
3. ActiveMatrix platform application should be updated to use the application template version rather than 3.4.0. For example, `com.tibco.amx.platform` Application.
4. From any host that has been downgraded, execute the following command from the `CONFIG_HOME\tibcohost\<HOST_NAME>\host\bin` folder to show the version history of the host or node. The last one should be the latest version and it should show the version that matches the version you downgraded to.

```
>tibcohost.exe describeHost
>tibcohost.exe describeNodes
```

This command shows the upgrade history along with other properties of the host which confirms that ActiveMatrix 3.4.0 is removed and host has been downgraded successfully.

5. All host and node executables will be downgraded and will display the earlier version of TIBCO Logo (only on Windows). Also, the `--version` command on the executable will show a version lower than 2.4.7.

## Using TIBCO Configuration Tool (TCT) to Upgrade or Downgrade

This section explains how you can use the following modes of TIBCO Configuration Tool (TCT) to Upgrade or Downgrade:

- GUI Mode
- Console Mode
- Silent Mode

It also explains how you can upgrade or downgrade using TCT-saved scripts.

## Diagnostic Tests

TIBCO Configuration Tool Wizard runs a set of tests on the selected `CONFIG_HOME` to check the eligibility for upgrade or downgrade. Most of the tests are common for both upgrade and downgrade. Some tests are specific to downgrade and are executed only when downgrading.



- If any of the tests fail, the TCT wizard will indicate that the CONFIG\_HOME is INELIGIBLE. It is recommended that the issues be addressed before proceeding with upgrade or downgrade. After fixing the issues, re-run the diagnostic tests.
- These diagnostic tests apply to the GUI mode and Console mode only.

## Tests That Are Common to Upgrade and Downgrade

### Validity of the Selected CONFIG\_HOME

The first of the tests verifies whether the specified CONFIG\_HOME is valid by checking the directory structure. If it does not meet the requirements, it is marked as INELIGIBLE and no further tests are executed.

### Disk Space Check

This test checks whether the specified CONFIG\_HOME has sufficient disk space so that upgrade or downgrade can be executed successfully.



At least 300MB of disk space is required for each host in the CONFIG\_HOME.



If test passes with success, the test details will show total disk space and free disk space in MB (megabytes) for the given CONFIG\_HOME.

### Disk Access Check

This test checks the read or write permission on the selected CONFIG\_HOME. A sample file (2MB) is used to copy to the specified CONFIG\_HOME for testing. If the CONFIG\_HOME is writable and takes less than 200 milliseconds, the test returns a SUCCESS.

### Runtime Host or Node Status

This test checks the runtime status of the hosts in the given CONFIG\_HOME. If any one of the hosts or nodes is found running, the test returns with a warning and a message with the number of hosts and nodes that are still in running state.

### Availability of Notification Server

This test checks the status of the notification server that is used by the enterprise. If the notification server is Running or if one of the servers in the Fault Tolerance (FT) pair is in the Running state, this test returns OK. If the notification server is not Running, a Failure is shown and the CONFIG\_HOME is marked as INELIGIBLE.



The notification server must be Running if you select the **Start Hosts** option in the Summary screen. If you are not starting the hosts, the notification server is not required to be in a Running state.

## Additional Tests for Downgrade

### Availability of ActiveMatrix Administrator

This test will check the availability for ActiveMatrix Administrator server. To downgrade successfully, ActiveMatrix Administrator is required to be running.

- **Success:** If an ActiveMatrix Administrator server is found to be running or one of the serve is running in case of replicated setup, test will display OK.
- **Warning:** If none of ActiveMatrix Administrators are available, the test returns Warning.



If you are downgrading CONFIG\_HOME that does not have ActiveMatrix Administrator (SystemHost), it is not required for ActiveMatrix Administrator to be running.



When downgrading ActiveMatrix Administrator host or SystemHost, ActiveMatrix Administrator server must be running before starting the downgrade process. Downgrade script will start ActiveMatrix Administrator server (if not running) automatically and then proceed with the downgrade.

### Availability of Old Platform Application Backup .zip Files

After hosts and nodes are downgraded, the next step involves reverting platform applications on each node. For this, the downgrade process needs old backup files that were created for each node during the upgrade. This test will check whether the backup files are available for downgrade.

- **Success:** If backup files for all nodes are found, the test returns OK.
- **Failure:** If any of backup files for nodes are missing, the test returns Failure.



Backup .zip files are located under `CONFIG_HOME\tibamx_hostmanager\OldPlatformAppsBackup\`.

## Using GUI Mode

See [Upgrade or Downgrade TIBCO ActiveMatrix](#) for more information on using the TCT GUI mode.

## Using Console Mode

As an example, these console windows show how to upgrade all the Hosts in an enterprise to ActiveMatrix 3.4.0. The procedure for downgrading in the console mode is the same.

1. In a console window, go to the `TIBCO_HOME\tct\1.6` directory and run the following command.

Platform	Description
Linux, UNIX	<code>TIBCOConfigurationTool -consoleMode</code>
Windows	<code>TIBCOConfigurationToolc.exe -consoleMode</code>

The following options appear.

```

Choose one option from the list below.

[X] 1 - Create Express Developer Environment - V3.4
[ ] 2 - Create TIBCO ActiveMatrix Administrator Server - V3.4
[ ] 3 - Create TIBCO ActiveMatrix Policy Director Administrator Server - V3.4
[ ] 4 - Create TIBCO ActiveMatrix Policy Director Proxy Host - V3.4
[ ] 5 - Create TIBCO Host Instance - V3.4
[ ] 6 - Configure Third-Party Driver
[ ] 7 - Edit TIBCO ActiveMatrix Administrator Server Configuration - V3.4
[ ] 8 - Replicate TIBCO ActiveMatrix Administrator Server - V3.4
[ ] 9 - Upgrade or Downgrade TIBCO ActiveMatrix - V3.4
[ ] 10 - Update JRE used by TIBCO ActiveMatrix - V3.4
[ ] 11 - Configure TIBCO Service Performance Manager - V2.3
[ ] 12 - Configure TIBCO ActiveMatrix SPM Dashboard - V3.4

To select an item enter its number, or enter 'q' to quit: [1] _

```

2. Select option 9 in the above screen to upgrade or downgrade and press **Enter**.

```

To select an item enter its number, or enter 'q' to quit: [1]9

=====
TIBCO ActiveMatrix Upgrade Manager
=====
Welcome to the TIBCO ActiveMatrix Upgrade Manager Wizard.

This wizard will help you to validate the CONFIG_HOME and upgrade to or downgrade from TIBCO ActiveMatrix 3.4.0

Choose 'N' for Next Page, 'L' for Load File, 'C' for Cancel, or enter field number [N]_

```

3. Type N (Next Page) to continue.

```

=====
TIBCO ActiveMatrix Upgrade Manager: Upgrade or Downgrade
=====
Select upgrade or downgrade.

[1] Upgrade: [yes]

This wizard will help you validate the CONFIG_HOME for a successful upgrade to ActiveMatrix 3.4.0,
and then upgrade all or a selection of Hosts to 3.4.0.
[2] Downgrade: [no]

This wizard will help you validate the CONFIG_HOME for a successful downgrade from ActiveMatrix 3.4.0,
and then downgrade all or a selection of Hosts from 3.4.0.

Choose 'N' for Next Page, 'P' for Previous Page, 'C' for Cancel, or enter field number [1] _

```

4. Type 1 to upgrade or 2 for downgrade and press **Enter**. In this example, let us select option 1 for upgrade.

```

=====
TIBCO ActiveMatrix Upgrade Manager: Upgrade Options
=====
Please select TIBCOHost(s) for upgrade.

[1] Upgrade All TIBCOHosts: [yes]
[2] Select TIBCOHosts to be upgraded: [no]

Note: Next screen will run diagnostic tests and it may take few moments to appear
[3] Skip diagnostic tests (not recommended): [no]

Choose 'N' for Next Page, 'P' for Previous Page, 'C' for Cancel, or enter field number [1]

```

5. Type 1 to upgrade all hosts or 2 to select a specific host to be upgraded and press **Enter**. In this example, let us select option 1 for upgrading all hosts. The diagnostic tests that are run are displayed. If any issues are found, (in this case: EMS server is not running), they are highlighted as a "WARNING".

The overall eligibility of the hosts to be upgraded is displayed as "ELIGIBLE" (in this case: as the EMS server need not be running for the upgrade process, it is considered as "ELIGIBLE").

```

=====
TIBCO ActiveMatrix Upgrade Manager: Validate
=====
The following aspects of your selected CONFIG_HOME were validated for the upcoming upgrade or downgrade.

Check for disk Space Availability CONFIG_HOME [E:/amxconfig/config_admin] - OK
    Total disk space: 10236 MB, Free space: 5225 MB
Disk copy speed test between TIBCO_HOME and CONFIG_HOME - OK
    Read / Write test succeeded, time took to copy 2 MB file : 62 ms
Check for TIBCOHost and Nodes Status in CONFIG_HOME [E:/amxconfig/config_admin] - OK
    Found 3 host(s) (0 are Running), Found 2 Node(s) (0 are Running) Warning: All running hosts and nodes must be st
opped before upgrade
Check for notification server(s) runtime status - WARNING
    None of the server(s) [tcp://amx-server-22:6777] found in notification.xml seems to be running .Host and Node st
artup may be affected

Eligibility status of CONFIG_HOME [E:/amxconfig/config_admin] - OK
ELIGIBLE

[1] Action "Rerun test(s)"
    Time taken to run test(s): 22 seconds
    Diagnostic report: [file:///E:/amxconfig/config_admin/tct/tct.upgrade.downgrade/2018-06-03-12-45-11/logs/upgrade_diagnosticTestResults.log]

Choose 'N' for Next Page, 'P' for Previous Page, 'C' for Cancel, or enter field number [1]_

```

6. For issues that were highlighted by the diagnostic test report, you can fix the issues and re-run the tests by selecting option 1 when prompted. For example, in the above case, you can start the EMS server and run the tests again. As shown below, the EMS test shows "OK" this time.

```

Choose 'N' for Next Page, 'P' for Previous Page, 'C' for Cancel, or enter field number [1]_
Action "Rerun test(s)"
Do you want to execute this action?: [yes]
The following aspects of your selected CONFIG_HOME were validated for the upcoming upgrade.

=====
TIBCO ActiveMatrix Upgrade Manager: Validate
=====
The following aspects of your selected CONFIG_HOME were validated for the upcoming upgrade or downgrade.

Check for disk Space Availability CONFIG_HOME [E:/amxconfig/config_admin] - OK
    Total disk space: 10236 MB, Free space: 5225 MB
Disk copy speed test between TIBCO_HOME and CONFIG_HOME - OK
    Read / Write test succeeded, time took to copy 2 MB file : 0 ms
Check for TIBCOHost and Nodes Status in CONFIG_HOME [E:/amxconfig/config_admin] - OK
    Found 3 host(s) (0 are Running), Found 2 Node(s) (0 are Running) Warning: All running hosts and nodes must be st
opped before upgrade
Check for notification server(s) runtime status - OK
    Found one of the notification server running

Eligibility status of CONFIG_HOME [E:/amxconfig/config_admin]:
ELIGIBLE

[1] Action "Rerun test(s)"
    Time taken to run test(s): 02 seconds
    Diagnostic report: [file:///E:/amxconfig/config_admin/tct/tct.upgrade.downgrade/2018-06-02-12-45-11/logs/upgrade_diagnosticTestResults.log]

Choose 'N' for Next Page, 'P' for Previous Page, 'C' for Cancel, or enter field number [1]_

```

7. The last screen shows a summary, as shown below.

```

Choose 'N' for Next Page, 'P' for Previous Page, 'C' for Cancel, or enter field number [1]N
=====
TIBCO ActiveMatrix Upgrade Manager: Upgrade Summary
=====
The following actions will be carried out on the selected TIBCOHost(s)

[1] Session Scripts and Log Folder: [E:\amxconfig\config_admin\tct\tct.upgrade.downgrade\2018-06-02-12-45-11]
Note: All Nodes managed by the TIBCOHost(s) will be upgraded automatically.
Note: Please back up the database before proceeding.
Note: Nodes will be stopped and started irrespective of startup mode.

[2] Stop ALL TIBCOHosts: [yes]
[3] Upgrade ALL TIBCOHosts: [yes]
[4] Perform post-upgrade tasks: [yes]
[5] Start ALL TIBCOHosts: [yes]

Choose 'P' for Previous Page, 'S' for Save, 'G' for Configure, 'C' for Cancel, or enter field number [1]_

```

8. After you review the pre-installation summary, type G to start the upgrade process. You can also select options to "Stop", "Upgrade", "Perform post-upgrade task" and "Start" by selecting the appropriate field number. When configuration completes, you can select a second configuration option or type q to quit.

A part of the output is shown below.



```

Choose 'P' for Previous Page, 'S' for Save, 'G' for Configure, 'C' for Cancel, or enter field number [1]G
Running target: [stop] for Host: [Admin-amxadmin-instanceOne]
ant -f build.xml stop

-check-build-properties:
[echo] loading tct build properties from E:\amxconfig\config_admin\tct\tct.upgrade.downgrade\2017-06-02-12-45-
1\scripts/build.properties

-load-build-properties:

-load-antcontrib:

-convert-build-properties-to-xml:
[mkdir] Created dir: E:\amxconfig\config_admin\tct\tct.upgrade.downgrade\2017-06-02-12-45-11\scripts\tmp

-init:

-define-patchmgr-tasks:

-test-targets.order:
[02 Jun 2018 12:56:23,154] Skipping build file 'ant target' order checking

do-stop:
[02 Jun 2018 12:56:23,154] Stop TIBCOHosts
Looking for Admin in Config Home: E:\amxconfig\config_admin
admin_bootstrap.properties path : E:\amxconfig\config_admin\admin\amxadmin\private\instanceOne
host.names.asCsv is Admin-amxadmin-instanceOne,RuntimeHost11,RuntimeHost12
Updating property file: E:\amxconfig\config_admin\tct\tct.upgrade.downgrade\2018-06-02-12-45-11\scripts\build.prope
ties
[02 Jun 2018 12:56:25,665] Stopping selected TIBCOHosts [Admin-amxadmin-instanceOne] in E:\amxconfig\config_admin
[02 Jun 2018 12:56:25,697] Executing command 'stopAllHosts' with arguments: -configHomeLocation E:\amxconfig\config_
admin -logFile E:\amxconfig\config_admin\tibamx_hostmanager\logs\tibamx_hostmanager.log -showTimeStamp
[02 Jun 2018 12:56:25,712] Following is the list of all tibcohost instances in config_home E:\amxconfig\config_admin
[02 Jun 2018 12:56:25,712] Admin-amxadmin-instanceOne
[02 Jun 2018 12:56:25,712]
[02 Jun 2018 12:56:25,712] Stopping ALL Host instances listed above

```



To select multiple Hosts for upgrading or downgrading, in the step 5 of the preceding procedure, type the numbers of the Hosts to be upgraded or downgraded separated by space (as shown in the following command prompt) and press **Enter**.

```

Administrator: C:\Windows\System32\cmd.exe - TIBCOConfigurationTool.exe -consoleMode
To select multiple item enter there number: [2][1][3]

Choose Select TIBCOHosts to be upgraded from the list below.

[ ] 1 - Admin-amxadmin-instanceOne <3.3.0>
[ ] 2 - RH1 <3.3.0>
[ ] 3 - RH3 <3.3.0>
[ ] 4 - RH2 <3.3.0>

To select multiple item enter there number: [1 2 3 4]

=====
TIBCO ActiveMatrix Upgrade Manager: Upgrade Selection
=====
Please select TIBCOHost(s) for upgrade.

[1] Select TIBCOHosts to be upgraded: [Admin-amxadmin-instanceOne RH1 RH3 RH2]
[X] - Admin-amxadmin-instanceOne <3.3.0>
[X] - RH1 <3.3.0>
[X] - RH3 <3.3.0>
[X] - RH2 <3.3.0>

```

## Using Silent Mode

TIBCO Configuration Tool (TCT) supports the silent mode where it takes the wizard ID and the build.properties as input files and runs TCT based on these files.

You can run TCT in the silent mode using the commands shown below. Note that the commands given below are for Windows and UNIX. For other operating systems, you will need to use the commands specific to the operating system.

Platform	Command
Linux, UNIX	TIBCOConfigurationTool -silentMode -wizard.id <i>wizard_id</i> - wizard.props <i>build_properties</i> [ <i>wizard.target ant_target-name</i> ]

Platform	Command
Windows	<code>TIBCOConfigurationToolc.exe -silentMode -wizard.id wizard_id -wizard.props build_properties [wizard.target ant_target-name]</code>

For example:

```
TIBCOConfigurationToolc.exe -silentMode -wizard.id
com.tibco.tct.amx.upgrade.downgrade -wizard.props
CONFIG_HOME\tct\tct.upgrade.downgrade\2018-06-12-13-20-10\scripts\build.properties
```

The wizard ID for the upgrade and downgrade wizard is : `com.tibco.tct.amx.upgrade.downgrade`.

The `wizard.props` points to the `build.properties` file created by TCT (GUI mode or Console mode). You can create it manually as well.



- The input file given in the `wizard.props` is not edited; it is copied and the new TCT folder structure gets created under the new location.
- This new location is picked up from property `tct.config.home` found in `TIBCOConfigurationToolc.ini`.
- By default, silent mode runs a default target found in `build.xml` and the current default target is `run.upgrade.downgrade`.
- If you do not need to run the default target, there is a `wizard.target` argument that you can pass in while starting silent mode.

## Using Scripts

In the Console mode and the GUI mode, the actions are recorded in the form of a script (`targets_config.bat` or `targets_config.sh`). This script can be modified and re-used later.

The last screen during upgrade or downgrade, that is, the Summary screen shows the location where the scripts are saved (**Session Scripts and Log Folder**). This folder contains a "Batch" script or a "Shell" script ( depending on the operating system) in the `scripts` folder.

You can double-click the batch file to run it. It starts executing whatever was selected during TCT screens.

In the Summary screen (GUI mode only), if you choose to skip any of the four actions ("Stop", "Upgrade", "Perform post-upgrade task" and "Start" Host) and save it, the `build.properties` file is updated to reflect this.

For example, if you choose to skip "Stop All Host" and skip "Start All Hosts", you will see two new properties added to the `build.properties` file.

```
skip.host.stop=true
skip.host.start=true
```

## ANT scripts

TCT at the end of the wizard creates a `build.xml` file that is the main ANT build file. Using this ANT file, TCT performs upgrade or downgrade. You can run this `build.xml` file manually as well.

The `build.xml` file takes its input from the `build.properties` file. Any upgrade or downgrade instructions or settings must be added to this file.

The `build.xml` also imports some other ANT build files needed to run upgrade or downgrade:

File	Description
<code>tct-tools.xml</code>	This is standard tct build file - have "-init" target in it.

File	Description
<code>patchmgr-task-3.4.0.xml</code>	This is an XML file that sets a CLASSPATH for running the Host Manager commands. Most of the upgrade and downgrade is performed by the Host manager located in <code>TIBCO_HOME\amx\3.4\bin</code> . ANT calls the Host manager using an ANT task. This file defines the ANT tasks and sets a CLASSPATH for them.
<code>tct-helper.xml</code>	This build file defines a code for many of the targets that are exposed in the top level <code>build.xml</code> . It defines <code>"do.run.upgrade.downgrade, do.stop, do.upgrade_downgrade"</code> and <code>do.post_upgrade</code> targets.
<code>process_form_apps.xml</code>	This build file is actually not used by the top-level <code>build.xml</code> file but rather used by <code>tct-helper.xml</code> . this build file defines targets that are needed for platform app upgrade or downgrade.

There are 5 main ANT targets:

ANT Target	Description
<code>run.upgrade.downgrade</code>	<p>Default target. This target performs Stop, Upgrade or Downgrade, post upgrade task, and Start for each host you have selected. Selection details are taken from the <code>build.properties</code> file.</p> <p>When this target is runs, it calls <code>do.stop, do.upgrade_downgrade, do.post_upgrade</code> and <code>do.start</code> sub-targets.</p>
Stop	<p>This target performs Stop on the selected host. The selection is taken from the <code>build.properties</code> file. Either <code>selectAll</code> is set to <code>true</code> (that is, all hosts in the <code>CONFIG_HOME</code>) or a comma-separated list of host names as the value for the property <code>upgrade.tibcohost/downgrade.tibcohost</code>). This target calls ANT taskdef <code>"patchmgr.StopAllHosts"</code> -calls the Host manager command (<code>./tibamx_hostmanager.exe stopAllHosts</code>).</p> <p>This target calls the <code>do</code> sub-target defined in <code>tct-helper.xml</code>.</p>



ANT Target	Description
upgrade_downgrade	<p>This target performs either upgrade or downgrade on the host. Selection is taken from <code>build.properties</code> file. Either property <code>selectAll</code> is set to <code>true</code> (that is, all Hosts in <code>CONFIG_HOME</code>) or comma-separated host names as value for the property <code>upgrade.tibcohost/downgrade.tibcohost</code>. This target calls ANT taskdef "patchmgr.Upgrade" or "patchmgr.Downgrade" - that calls the Host manager command (<code>tibamx_hostmanager.exe upgradetibamx_hostmanager.exe downgrade</code>). This target calls the <code>do.upgrade_downgrade</code> sub-target that is defined in <code>tct-helper.xml</code>.</p> <p>This target has the following sub-targets that can be called before <code>run.upgrade_downgrade</code> and it enables you to skip certain actions:</p> <ul style="list-style-type: none"> <li>• <code>skip.host.start</code>: skip host start</li> <li>• <code>skip.host.stop</code>: skip host stop</li> <li>• <code>skip.upgrade.or.Downgrade</code>: skip host upgrade or downgrade ( based on <code>build.properties</code> input)</li> <li>• <code>skip.post.upgrade</code>: skip post upgrade</li> </ul> <p>For example:</p> <pre>ant -f skip.host.start run.upgrade_downgrade</pre> <pre>ant -f skip.upgrade.or.Downgrade skip.post.upgrade run.upgrade_downgrade</pre>
start	<p>This target performs "Start" on the selected host. The selection is taken from the <code>build.properties</code> file. Either property <code>selectAll</code> is set to <code>true</code> (that is, all hosts in the <code>CONFIG_HOME</code>) or a comma-separated list of host names as value for the property <code>upgrade.tibcohost/downgrade.tibcohost</code>. This target calls ANT taskdef "patchmgr.StartAllHosts" - that calls the Host manager command (<code>./tibamx_hostmanager.exe startAllHosts</code>).</p> <p>This target calls <code>do.start</code> sub-target that is defined in <code>tct-helper.xml</code>.</p>
post.upgrade	<p>This target performs a "post-upgrade" action during the upgrade process. This target also calls ANT taskdef "patchmgr.UpdateManifest" - that calls the Host manager command (<code>./tibamx_hostmanager.exe updateManifest</code>). This target calls <code>do.post.upgrade</code> sub-target defined in <code>tct-helper.xml</code>. This target is only relevant during the upgrade action (in <code>build.properties</code> file <code>isUpgrade</code> is set to <code>true</code>.)</p>



If you want to perform only the target action (such as `STOP`), you can select a host or all hosts in the given `CONFIG_HOME` and call individual targets like "stop" defined in `build.xml`. If you want to perform `stop`, `upgrade/downgrade`, `post upgrade` and `start` on the selected host, it is recommended that you call the `run.upgrade_downgrade` target.



Upgrading by executing the scripts manually and by executing them through the TCT Wizard are different. TCT performs additional sequencing which cannot be done by the ANT scripts.

Is "ant -f build.xml stopupgrade\_downgrade post.upgrade start" the same as "ant -f build.xml run.upgrade.downgrade" ?

No. If you call targets "stop upgrade\_downgrade post.upgrade start", ANT calls each target one after the other. For example, consider 3 hosts in a CONFIG\_HOME. If you call targets described as before, ANT calls the stop target first and it stops all 3 hosts. Then, it calls the upgrade\_downgrade target and performs either upgrade or downgrade depending on the input selected in the build.properties file for all 3 hosts. Then, it performs the post.upgrade followed by calling the start target.

### Sample Output - Success

```
[11 Jun 2018 18:02:31,420]
~~~~~
#Ant properties
#Sun Jun 11 18:02:31 PDT 2018
tibco.host.Admin-dev-enterprise-instanceOne.Downgrade.status=SUCCESS
tibco.host.RunTimeHost.Downgrade.status=SUCCESS
tibco.host.RunTimeHost11.Downgrade.status=SUCCESS
tibco.host.RunTimeHost2.Downgrade.status=SUCCESS
tibco.host.RunTimeHost3.Downgrade.status=SUCCESS
tibco.host.RunTimeHost4.Downgrade.status=SUCCESS
tibco.host.RunTimeHost5.Downgrade.status=SUCCESS
tibco.host.RunTimeHost6.Downgrade.status=SUCCESS
tibco.host.RunTimeHost7.Downgrade.status=SUCCESS
tibco.host.RunTimeHost8.Downgrade.status=SUCCESS
tibco.host.RunTimeHost9.Downgrade.status=SUCCESS
[11 Jun 2018 18:02:31,422]
~~~~~
```

### Sample Output - Failure

```
[12 Jun 2018 13:44:29,636]
~~~~~
#Ant properties
#Mon Jun 12 13:44:29 PDT 2018
tibco.host.RuntimeHost3.Upgrade.status=FAILURE
tibco.host.RuntimeHost3.Upgrade.status.error=The following error occurred while
executing this line\:r\nC:\\tibco_amx331_for_340\\amx\\3.4\\scripts\\upgrade\\
\\upgrade-to-3.4.0\\platformApp\\tct-helper.xml\:316\: The following error occurred
while executing this line\:r\nC:\\tibco_amx331_for_340\\amx\\3.4\\scripts\\upgrade
\\upgrade-to-3.4.0\\platformApp\\tct-helper.xml\:328\: The following error occurred
while executing this line\:r\nC:\\tibco_amx331_for_340\\amx\\3.4\\scripts\\upgrade
\\upgrade-to-3.4.0\\platformApp\\process_platform_apps.xml\:237\: The following
error occurred while executing this line\:r\nC:\\tibco_amx331_for_340\\amx\\3.4\\
\\scripts\\upgrade\\upgrade-to-3.4.0\\platformApp\\process_platform_apps.xml\:275\:
One of the nodes failed to perform upgrade of platform App - please check logs at
\: E:\\amxconfig\\config_331_RuntimeHost2\\tct\\tct.upgrade.downgrade\\
\\2018-06-12-13-20-10\\logs\\platformApp.logs\\12-
Jun-2018-13_43_40.updatePlatformApp.admin.cmdline.log for more information
tibco.host.RuntimeHost4.Upgrade.status=FAILURE
tibco.host.RuntimeHost4.Upgrade.status.error=The following error occurred while
executing this line\:r\nC:\\tibco_amx331_for_340\\amx\\3.4\\scripts\\upgrade\\
\\upgrade-to-3.4.0\\platformApp\\tct-helper.xml\:242\: TIBCO-AMX-TOOLS-
PATCHMGR-000601\: One or more Host instances have not started or they are still
starting. Make sure all Host instances have started. Start a Host instance manually
if it has not started.
[12 Jun 2018 13:44:29,652]
~~~~~
```

## Upgrading and Downgrading: An Example

This section explains the upgrade and downgrade process using a sample instance. Screenshots of some of the TCT wizard screens are provided in the respective workflows.

## Instance Details

For this example, consider that a machine contains 3 hosts: Admin-amxadmin-instanceOne, RuntimeHost11, and RuntimeHost12.

In this example:

- TIBCO\_HOME refers to the directory where you installed ActiveMatrix 3.4.0 using the TIBCO Universal Installer.
- CONFIG\_HOME refers to the directory where you created or configured your enterprise using TIBCO Configuration Tool (TCT). For example, C:/amx.home/data.

The following UI shows a list of hosts and nodes before the upgrade:

**Hosts**

Machine: All

Name	Version	Host State	Machine	Action History
SystemHost	3.3.0.HF15	Running	apcWin2k8R2x64-55	<a href="#">Install features successful</a>
RuntimeHost12	3.3.0.HF15	Running	apcWin2k8R2x64-55	<a href="#">Bind Successful</a>
RuntimeHost11	3.3.0.HF15	Running	apcWin2k8R2x64-55	<a href="#">Bind Successful</a>

**Nodes**

Name	Host	Machine	Node State	Version	Synchronization	Startup Mode	Action History
DevNode	SystemHost	10.108.80.120	Running	3.3.0.HF15	In Sync	Automatic	<a href="#">Change features successful</a>
DevNodeHost1Node1	RuntimeHost1	10.108.80.120	Running	3.3.0.HF15	In Sync	Automatic	<a href="#">Change features successful</a>
DevNodeHost1Node2	RuntimeHost1	10.108.80.120	Running	3.3.0.HF15	In Sync	Automatic	<a href="#">Change features successful</a>
DevNodeHost2Node3	RuntimeHost2	10.108.80.120	Running	3.3.0.HF15	In Sync	Automatic	<a href="#">Change features successful</a>
DevNodeHost2Node4	RuntimeHost2	10.108.80.120	Running	3.3.0.HF15	In Sync	Automatic	<a href="#">Change features successful</a>

The following UI shows the applications running on the DevEnvironment:

**Applications**

Environment: DevEnvironment

Name	Application State	Last Deployed On	Synchronization	Action History
System				
amx.platform.apps				
com.tibco.amx.platform (DevNode)	Running	2019-01-08 12:26:27	In Sync	<a href="#">Platform Install Successful</a>
com.tibco.amx.platform (ProxyNode)	Running	2019-01-08 12:29:59	In Sync	<a href="#">Platform Install Successful</a>
com.tibco.amx.it.mediation.apt	Running	2019-01-08 12:30:35	In Sync	<a href="#">Deploy with Start Successful</a>
HelloWorld-1	Running	2019-01-08 12:30:51	In Sync	<a href="#">Deploy with Start Successful</a>

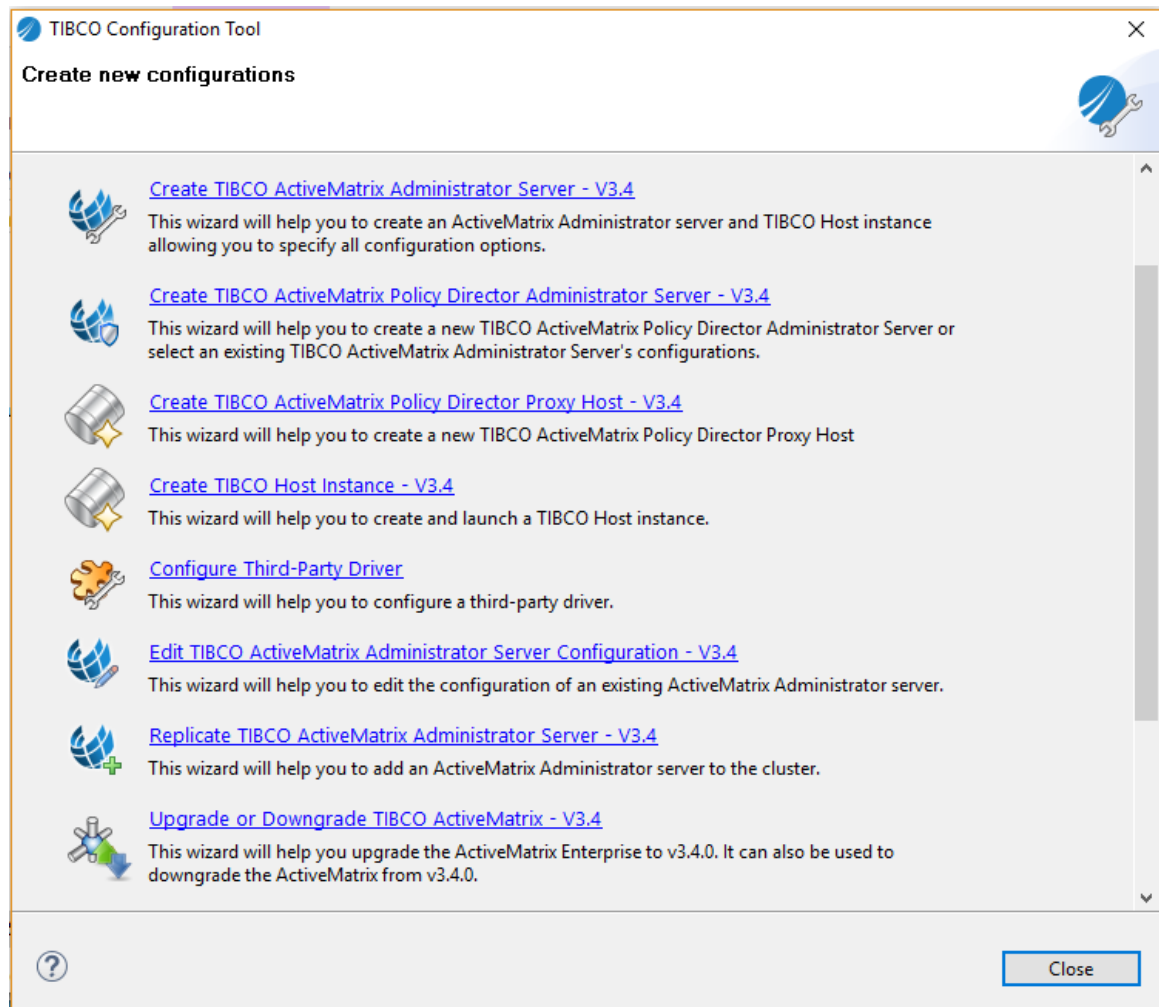
In the following section, we will upgrade Admin-amxadmin-instanceOne, RuntimeHost11, and RuntimeHost12.

## Upgrading Using TCT Wizard

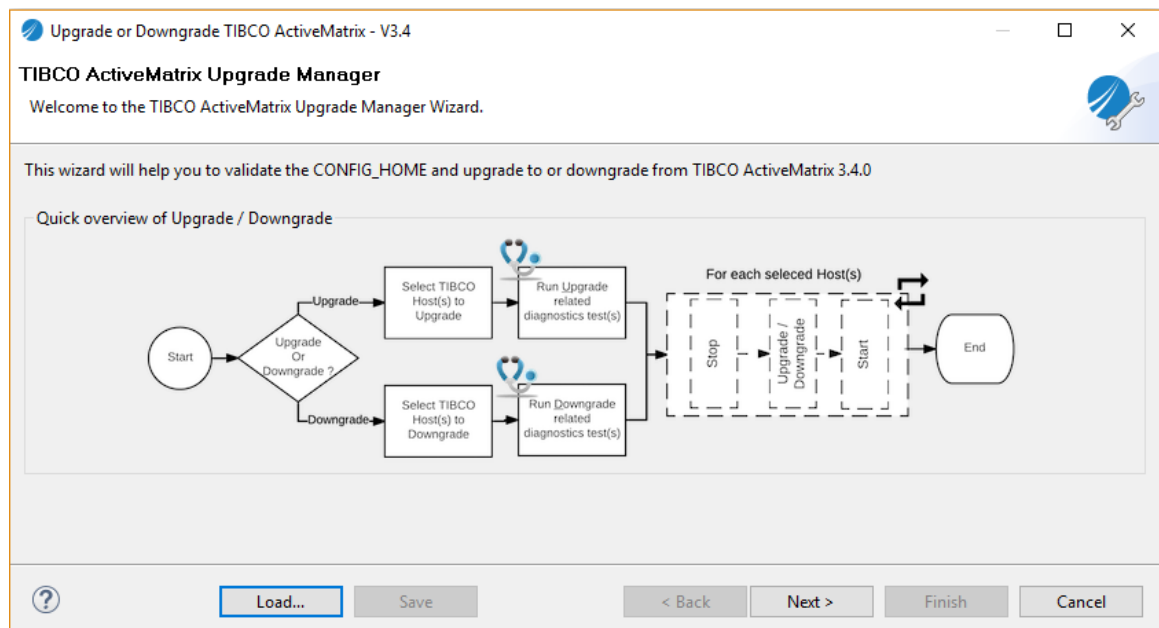
### Upgrading the ActiveMatrix Administrator Instance

After installing ActiveMatrix 3.4.0 on TIBCO\_HOME:

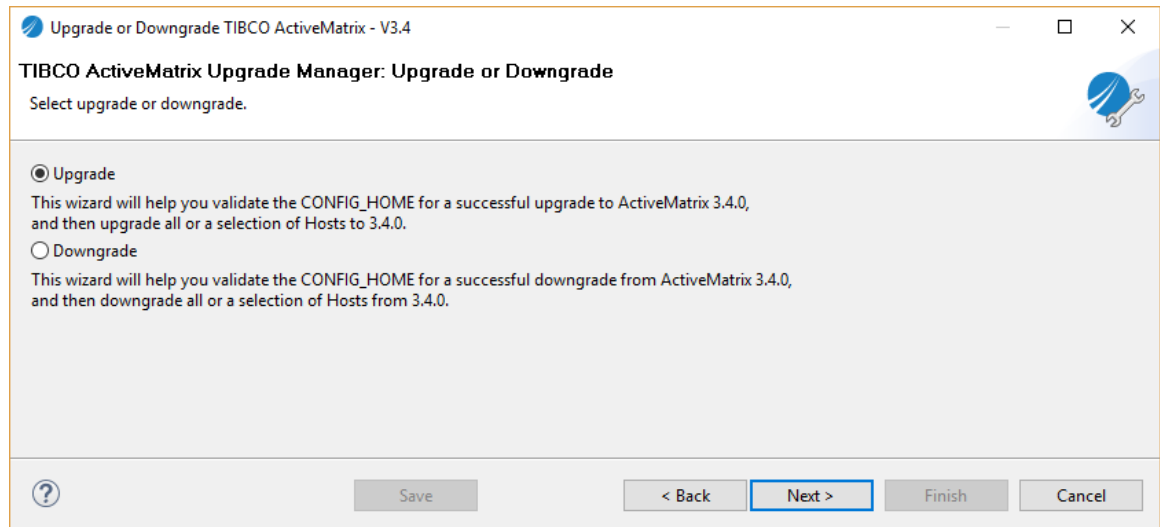
1. Navigate to TIBCO\_HOME/tct/1.6 and start the TCT wizard by running the TIBCOConfigurationTool.exe.
2. Select the CONFIG\_HOME to be upgraded. In this case, select the CONFIG\_HOME where the Administrator Server is running (for example: C:\amx.home\data).
3. Click **OK**.



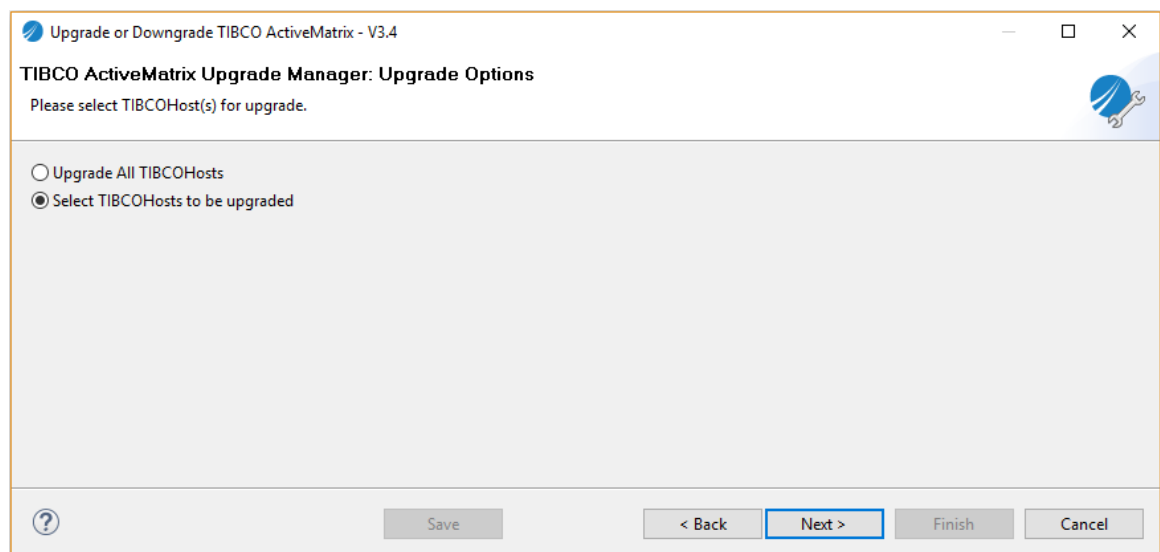
4. Select **Upgrade or Downgrade TIBCO ActiveMatrix - V3.4**. The overview workflow of both upgrade and downgrade path is displayed.



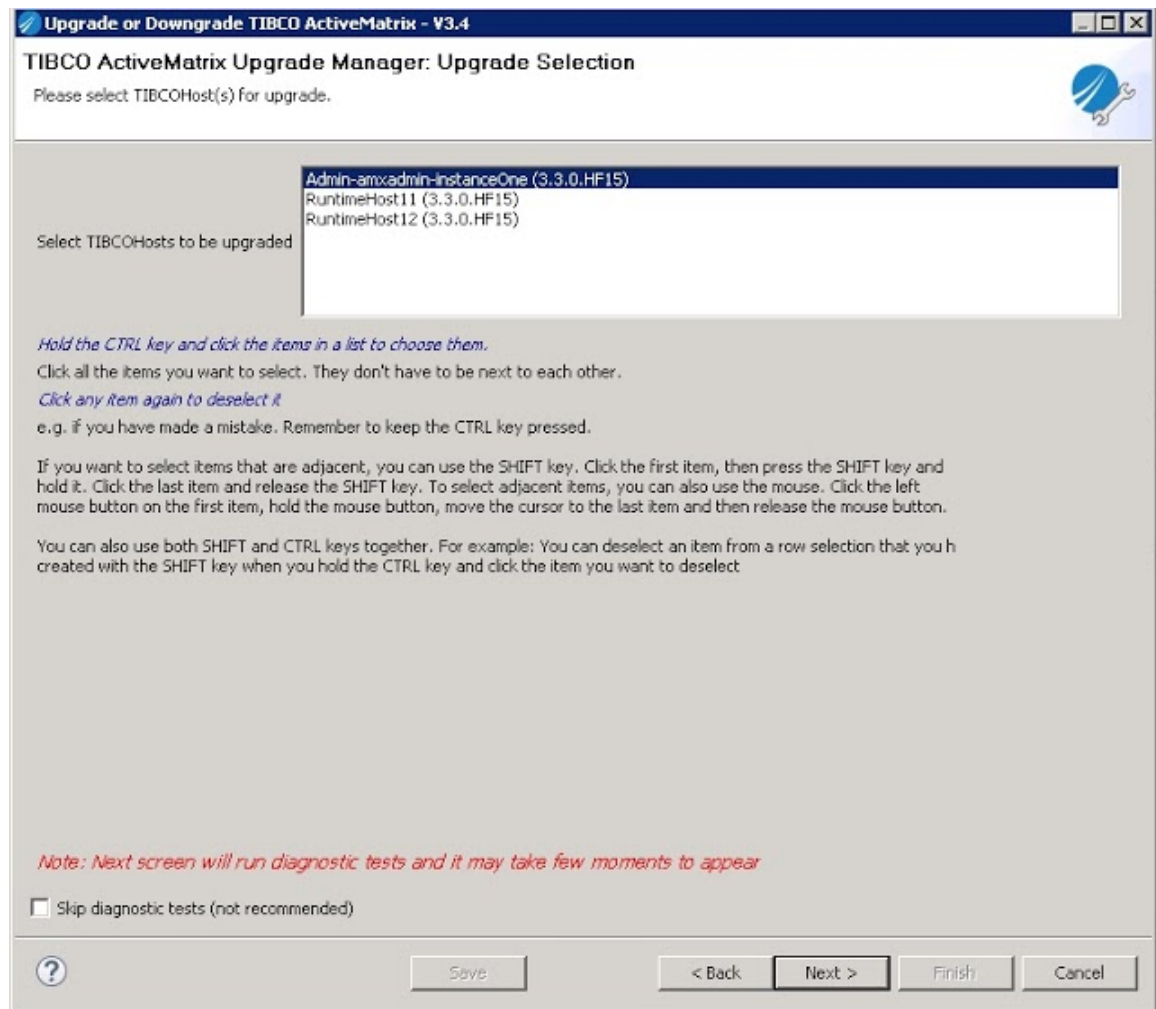
5. Click **Next**.



6. Select **Upgrade** and click **Next**.



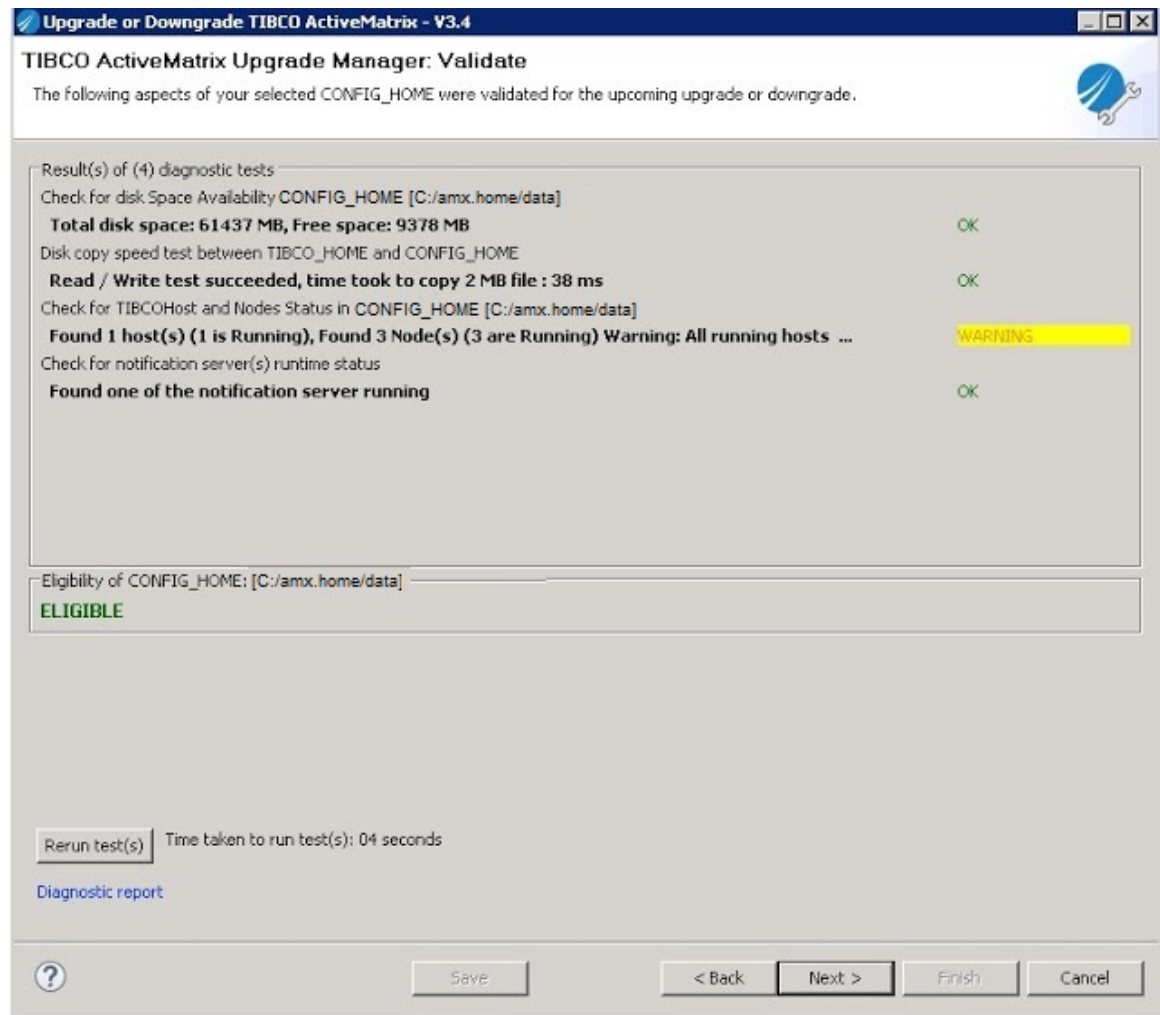
7. Select **TIBCOHosts to be upgraded** to select specific Hosts for upgrading or select **Upgrade All TIBCOHosts** to upgrade all hosts in the CONFIG\_HOME. In this example, select **Select TIBCOHosts to be upgraded** option and click **Next**.



This screen displays the list of hosts to be selected for upgrade. Select **Admin-amxadmin-instanceOne** from the list and click **Next**.

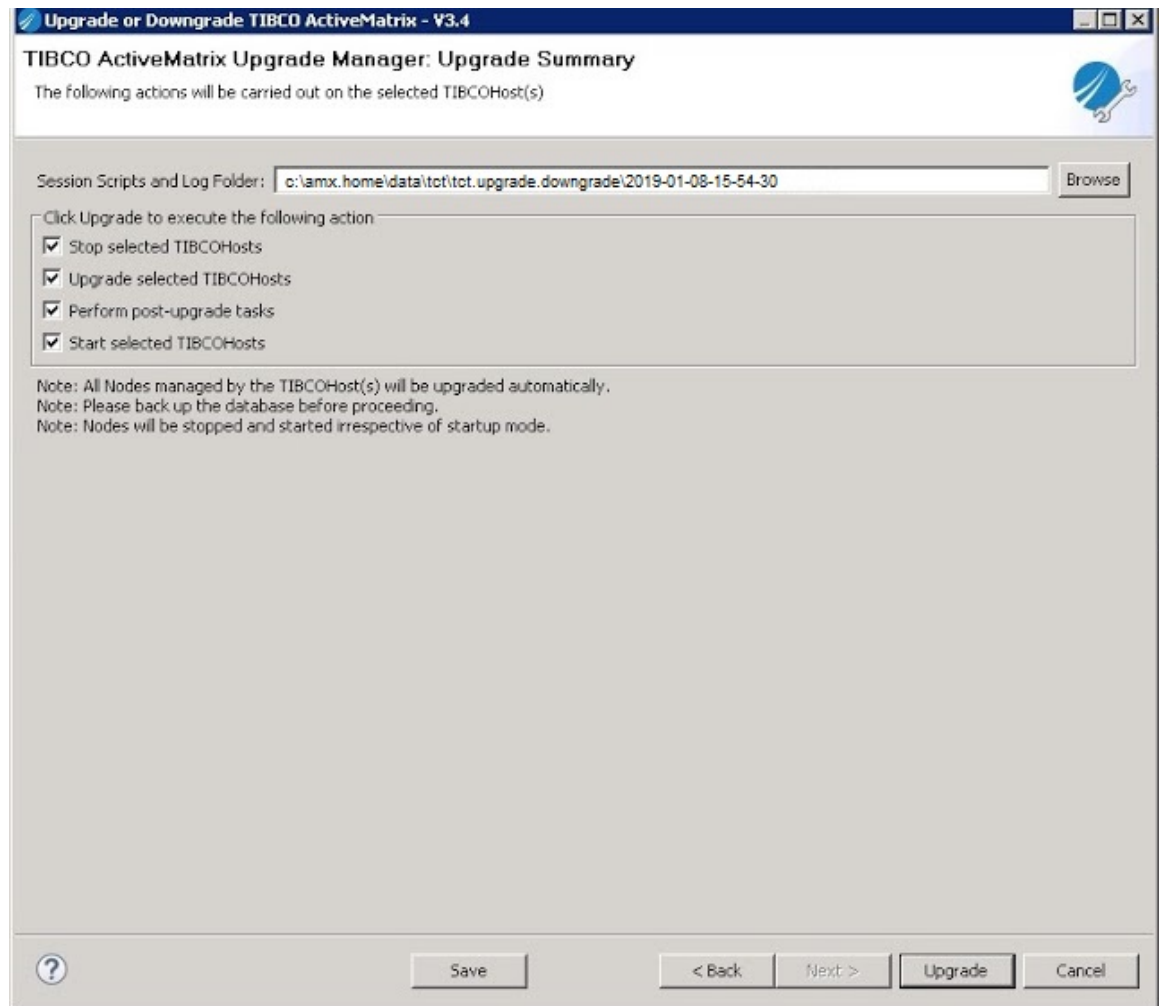


If you want to upgrade selective hosts, the Administrator instance must be upgraded first before the other hosts to be upgraded. If the list has Administrator, it will be upgraded first.



On this screen, TCT runs some diagnostic tests on the selected CONFIG\_HOME. The screen shows whether the selected CONFIG\_HOME is **ELIGIBLE** for an upgrade. Warnings are highlighted. You can also re-run the tests after the errors highlighted by the warnings are fixed.

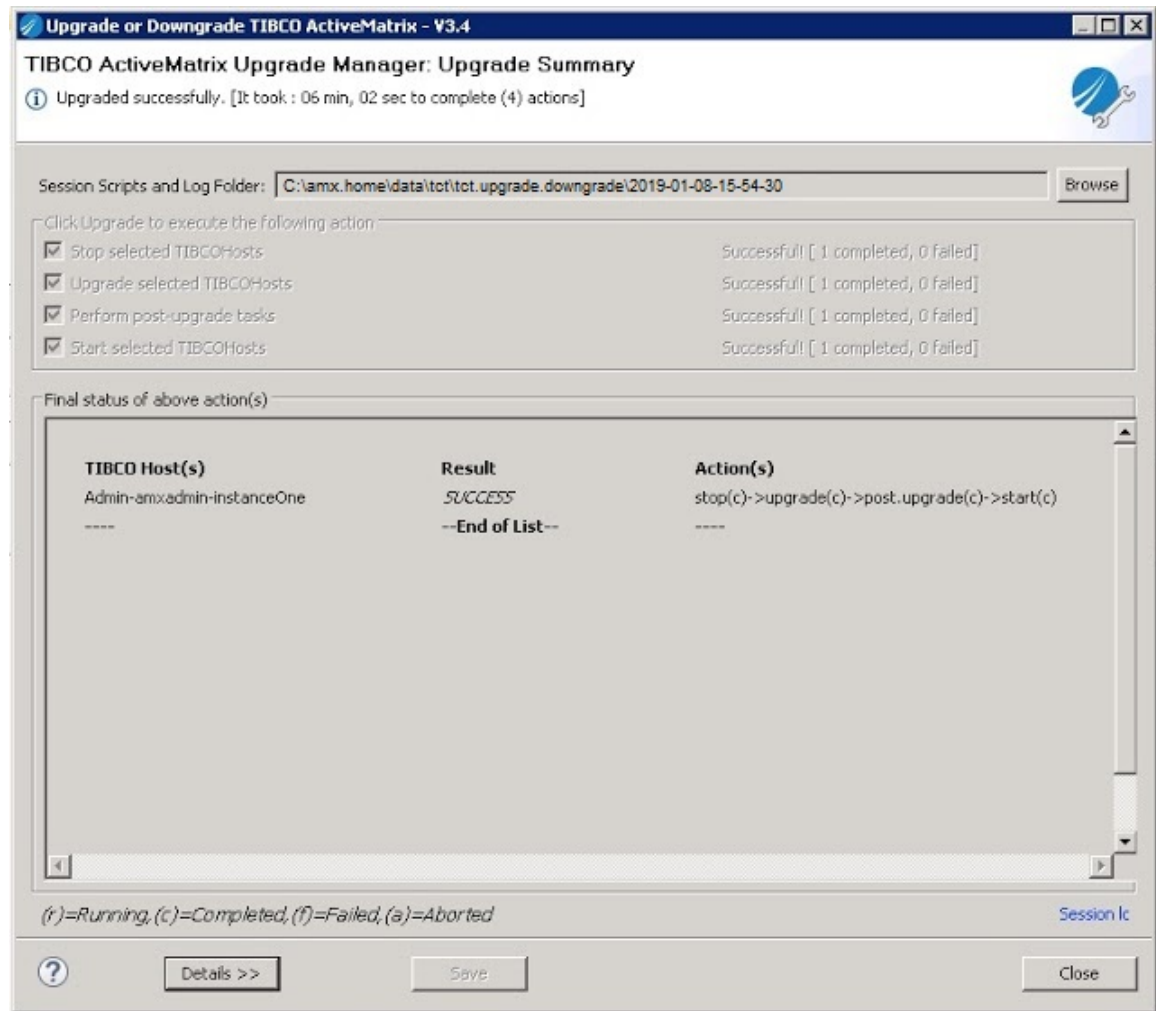
8. Click **Next**.



This screen shows a summary and a list of actions to be performed while upgrading the selected hosts.

9. Click **Upgrade**. This will perform the actions listed to upgrade the selected Hosts and returns a summary as shown below. Execution logs and scripts are also stored under the folder listed in the **Session Scripts and Log Folder** location.





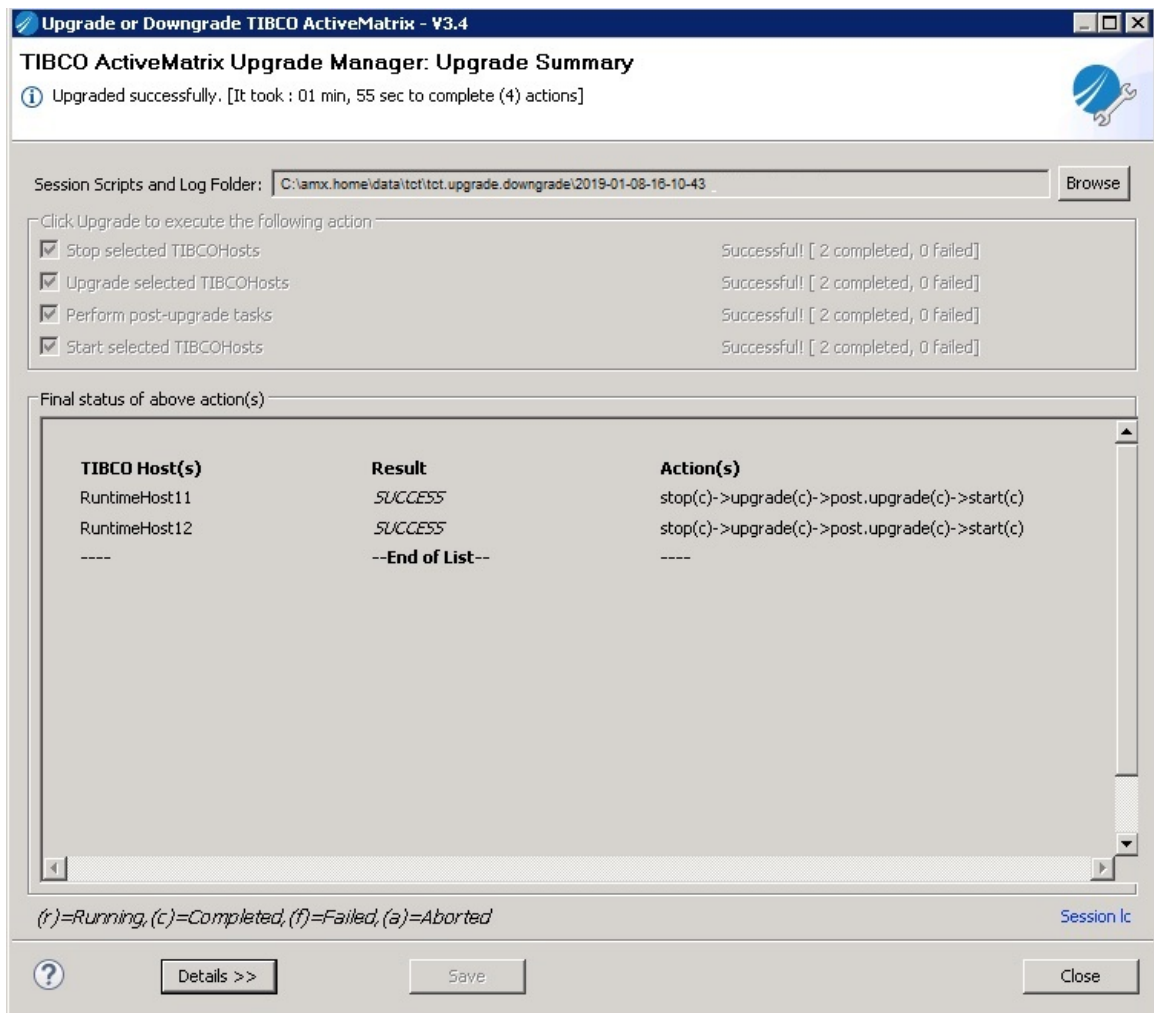
10. Click Close.

## Upgrading Runtime Hosts

As mentioned earlier, when upgrading, ActiveMatrix Administrator host or SystemHost must be upgraded *first*. That is, before upgrading any runtime host and node.

The steps to upgrade runtime hosts are similar to upgrading the ActiveMatrix Administrator Instance.

After all the runtime hosts are upgraded, the Summary screen should look like the following:



### Summary Screen

The Summary screen shows detailed information regarding the upgrade progress.

The screen shows a table containing the list of hosts, result of upgrade and actions with status. When all the actions are completed successfully without any failure, **SUCCESS** is displayed in the **Result** column of the host. If any action fails, the **Result** column shows **FAILURE**. You can also check the status of each action in the **Action(s)** column, beside the name of the action. One of the following statuses is displayed beside the action name:

- Running (**r**): Actions is currently running or being executed
- Completed (**c**): Action is completed successfully
- Failed (**f**): Action is completed with failure
- Aborted (**a**): Action is skipped or aborted

After the upgrade is completed, the total time taken for the upgrade is displayed on the top of the Summary screen immediately below the title.

### Verifying Upgrade

After upgrading to the current release, you can use the following methods to verify whether the Hosts, Nodes and System Applications are upgraded successfully and to check whether they are using the new version.

## Checking Host and Node Version from the ActiveMatrix Administrator UI

After upgrading to 3.4.0, all Hosts that are upgraded show the new version in the **Version** column of the **Infrastructure > Hosts** screen in the ActiveMatrix Administrator UI.

Name	Version	Synchronization Status	Host State	Machine	Action History
SystemHost	3.4.0	In Sync	Running	WIN-CL2.amx.tibco.com	Uninstall features successful
RuntimeHost11	3.4.0	In Sync	Installed	WIN-CL2.amx.tibco.com	Install Successful
RuntimeHost12	3.4.0	In Sync	Installed	WIN-CL2.amx.tibco.com	Paused Offline (4)

After upgrading to 3.4.0, all the Nodes that are upgraded show the new version in the **Version** column of the **Infrastructure > Nodes** screen in the ActiveMatrix Administrator UI.

Name	Host	Machine	Node State	Node Health	Version	Synchronization	Startup Mode	Action History
DevNode	SystemHost	WIN-CL2.amx.tibco.com	Running	Not healthy	3.4.0	Out of sync	Automatic	Change features successful
DevNode1Host11	RuntimeHost11	WIN-CL2.amx.tibco.com	Not installed	Unknown	3.4.0	Out of sync	Automatic	
DevNode1Host12	RuntimeHost12	WIN-CL2.amx.tibco.com	Not running	Unknown	3.4.0	In Sync	Automatic	Paused Offline (3)

## Checking Host and Node Version from the Command Line

The Host version can be verified from the command line using the `TIBCO_HOME/amx/<version>/bin/tibamx_hostmanager.exe describeHostUpgradeHistory` or using the `host/bin/tibcoHost.exe describeHost` command.

An example using the `tibamx_hostmanager.exe describeHostUpgradeHistory` command is shown below.

Command:

```
tibamx_hostmanager.exe describeHostUpgradeHistory -configHomeLocation C:\amx.home\data -instanceName Admin-amxadmin-instanceOne
```

Output:

```
Invoking describeHostUpgradeHistory
-configHomeLocation C:\amx.home\data
-instanceName Admin-amxadmin-instanceOne
```

Upgrade history, current to oldest:

```
Host platform version: 3.4.0, associated patch(es): amx.platform.patch:3.4.0
Host platform version: 3.3.0.HF15, associated patch(es):
amx.platform.patch:3.3.0.HF15
Host platform version: 3.3.0, no associated patch(es)
Host can be Downgraded:
3.3.0.HF15
```

Using `tibcoHost.exe describeHost` command:

Command:

```
tibcohost.exe describeHost
```

Output:

```
Invoking describeHost
```

Host description follows:

```
Host name: SystemHost
Enterprise name: amxadmin
HPA instance name: Admin-amxadmin-instanceOne
Bind status: bound
Internet host name: apcWin2k8R2x64-55
HPA type: TibcoHost
HPA specification version: 2.2.0
```

```

Host platform version: 3.4.0
Connect URL: service:jmx:jmxmp://apcWin2k8R2x64-55:6051
O/S name: Windows Server 2008 R2
O/S version: 6.1
O/S process ID: 7424
System architecture: amd64
Secure connection: false
Patch(es) associated with this version:
Upgrade history, current to oldest:
    Host platform version: 3.4.0, associated patch(es): amx.platform.patch:3.4.0
    Host platform version: 3.3.0.HF15, associated patch(es):
amx.platform.patch:3.3.0.HF15
    Host platform version: 3.3.0, no associated patch(es)
Upgrade status: none

```

Using tibcoHost.exe describeNodes command:

Command:

```
tibcohost.exe describeNodes
```

Output:

```

Invoking describeNodes

Description of node "DevNode" follows:
  Node description: Development node
  Current status: RUNNING
  Node type: com.tibco.amf.hpa.tibcohost.node.hibernate.feature
  Node type version: 3.4.0
  Platform version: 3.4.0
  Start mode: auto
Description of node "ProxyNode" follows:
  Node description: ProxyNode
  Current status: RUNNING
  Node type: com.tibco.amf.hpa.tibcohost.node.hibernate.feature
  Node type version: 3.4.0
  Platform version: 3.4.0
  Start mode: auto
Description of node "SystemNode" follows:
  Node description: Admin Default Node
  Current status: RUNNING
  Node type: com.tibco.amf.hpa.tibcohost.node.hibernate.feature
  Node type version: 3.4.0
  Platform version: 3.4.0
  Start mode: auto

```

### Checking Node Logs for New Version

After upgrading, when the Node is started, look for the following log lines at the beginning of the Node log. It shows the version of TIBCO ActiveMatrix that the Node is running. Here is an example from the SystemNode.log.

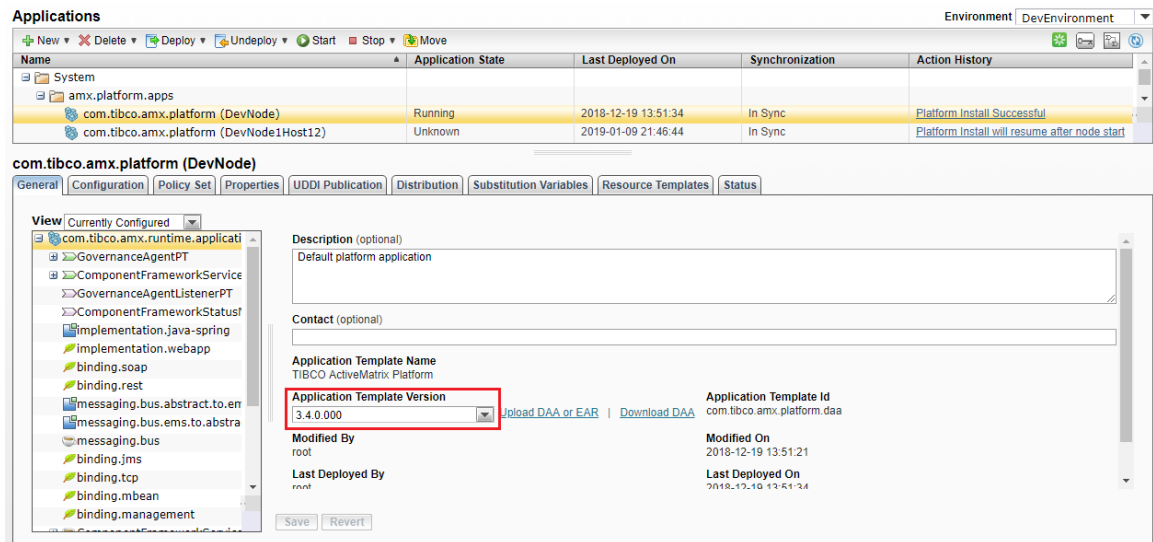
```

com.tibco.amx.hpa.node.Node - %%%%%%%%%%
%%%%%%%%%
com.tibco.amx.hpa.node.Node - TIBCO-AMX-HPA-014681: node "SystemNode" is running
version 3.4.0 of TIBCO ActiveMatrix Platform
com.tibco.amx.hpa.node.Node - %%%%%%%%%%
%%%%%%%%%

```

### Checking Platform Application Version

After upgrading to ActiveMatrix 3.4.0, the platform application (com.tibco.amx.platform) version is changed to 3.4.000. This can be verified from the **Applications** screen of the ActiveMatrix Administrator UI.



Also, check whether all the Applications are in the Running state.

## Analyzing the Upgrade Logs

This section describes the logs and provides log samples which helps to understand different stages of the Upgrade process.

TCT logs are stored in the `logs` folder under the path mentioned in the **Session Scripts and Logs Folder** in the Summary screen.

You can see that the entire TCT console logs are available in one file (`tct.console.output.TIMESTAMP.log`) and also the logs of each actions in a separate log files (that is, 4 log files for the corresponding actions of each Host).

## Start and Stop Action Logs

Start and stop action logs are simple and shows the console output of the start and stop commands of the Host.

## Upgrade Action Logs

Upgrade logs contain detailed information about the Upgrade process. The [Upgrade](#) section describes all the steps related to the Upgrade process in detail. The following are examples (headers and sample log) from the upgrade logs corresponding to each step in the Upgrade process.

1. **Installing Product Features on a Host:** This can be verified under the following header.

```
-----
Installing product features for version : 3.4.0
-----

-----
Following product features will be INSTALLED on host
-----
```

2. **Enabling Product Features on Node:** Corresponding log entries can be found under the following header.

```
-----
Enabling product features on nodes
-----

-----
Following product features will be ENABLED on node :SystemNode
-----
```

3. **Disabling old Product Features:** Corresponding log entries can be found under the following header which contains the list of product features that are disabled on the node.

```
-----
Following product features will be DISABLED on node :SystemNode
-----
```

4. **Upgrading Wrappers Logs**

```
Updating wrappers for the Host instances and Nodes
Updating wrapper for the Host instance: Admin-amxadmin-instanceOne
Successfully updated wrapper for the Host instance: Admin-amxadmin-instanceOne
Updating wrapper for Nodes on Host instance: Admin-amxadmin-instanceOne
Updating wrapper for the Node: DevNode
Successfully updated wrapper for the Node: DevNode
Updating wrapper for the Node: SystemNode
Successfully updated wrapper for the Node: SystemNode
```

5. **Upgrading Platform Application and REST Binding System Application:** Logs for upgrading platform application and removing the add-on REST Binding System Applications can be seen under the following header.

```
print-report-start-process:
[19 Jul 2017 19:13:27,578] Doing upgrade
[19 Jul 2017 19:13:27,578] AMX Node(s): [DevNode,SystemNode] found in
CONFIG_HOME [C:\amx.home\data\config_admin\tibcohost\Admin-amxadmin-instanceOne]

*****
*****
This script will upgrade all node's AMX Platform Application listed below
Total Nodes to process: 2
Node: DevNode
Node: SystemNode
Tibco Home for this AMX Nodes is: C:\tibco
Configuration Home for this AMX Nodes is: C:\amx.home\data\config_admin\tibcohost
\Admin-amxadmin-instanceOne
Tibcohost name is : Admin-amxadmin-instanceOne

*****
*****
```

6. **Summary:** Once the applications are upgraded, it prints a summary of the result as follows.

```
#####
#####
##### Report of platform App upgrade for each node in CONFIG_HOME : C:\amx.home
\data\
#####
#####
#Ant properties
#Wed Jul 19 19:16:06 PDT 2017
Admin-amxadmin-instanceOne.node.DevNode=SUCCESS
Admin-amxadmin-instanceOne.node.DevNode.timetaken=1\:17.010 sec
Admin-amxadmin-instanceOne.node.SystemNode=SUCCESS
Admin-amxadmin-instanceOne.node.SystemNode.timetaken=1\:19.559 sec
#####
#####
```

## Post Upgrade Action Logs

Post upgrade action involves updating the package dependency of the dashboard client application and updating the dependency range of the javax.servlet package on all the applications using it to make it compatible with the new Jetty version.

Following log samples capture the post upgrade action where it updates the Dashboard client dependency:

```
Updating the manifest for following instance : "Admin-amxadmin-instanceOne"
INFO: Updating the bundles in Node name: "DevNode"
The Manifest Updater searching in the directory : 'C:\amx.home\data\tibcohost
\Admin-amxadmin-instanceOne\data_3.2.x\nodes\DevNode\work\cf'
```

```

INFO: Updating the bundles in Node name: "SystemNode"
The Manifest Updater searching in the directory : 'C:\amx.home\data\tibcohost\
Admin-amxadmin-instanceOne\data_3.2.x\nodes\SystemNode\work\cf'

The Component Details
Application name : 'com.tibco.amx.platform.dashboard'
Component Name : 'DashBoardWebApp'
Component ID : '76d6dc95-3fc2-4a8f-a941-93f8cd15a16a'
Component Path : 'C:\amx.home\data\tibcohost\Admin-amxadmin-instanceOne
\data_3.2.x\nodes\SystemNode\work\cf\76d6dc95-3fc2-4a8f-a941-93f8cd15a16a'
Before com.tibco.amx.dashboard.client version = [1.0.0,1.0.100)
After com.tibco.amx.dashboard.client version = [1.0.0,2.0.0)
INFO: Bundle file updated of location : 'C:\amx.home\data\tibcohost\Admin-
amxadmin-instanceOne\data_3.2.x\nodes\SystemNode\work\cf\76d6dc95-3fc2-4a8f-
a941-93f8cd15a16a\bundle'

```

Following log samples capture the post upgrade action where it updates the dependency of the javax.servlet package of the Artifact Server Application.

```

INFO: Updating the bundles in Node name: "SystemNode"
The Manifest Updater searching in the directory : 'C:\amx.home\data\tibcohost\
Admin-amxadmin-instanceOne\data_3.2.x\nodes\SystemNode\work\cf'
The Component Details
Application name : 'com.tibco.amx.platform.artifactserver'
Component Name : 'ArtifactServer'
Component ID : '911ff791-ea69-4de0-b939-fb41b7744c61'
Component Path : 'C:\amx.home\data\tibcohost\
Admin-amxadmin-instanceOne\data_3.2.x\nodes\SystemNode\work\cf\911ff791-ea69-4de0-
b939-fb41b7744c61'

Before javax.servlet.http version = [2.5.100,4.0.0)
After javax.servlet.http version = [2.5.100,4.0.0)

```

Finally, the logs to clear the cache of the Nodes are displayed as follows.

```

Performing clear cache on the Host instances
Clearing cache of all Nodes of Host instance: Admin-amxadmin-instanceOne
Clearing cache for the Node: DevNode
Clearing cache for the Node: SystemNode

```

## SystemNode Upgrade Logs

After the Runtime is upgraded, ActiveMatrix Administrator updates the database with the data from Runtime to make it in sync. Here are some examples from the SystemNode log which show these updates.

- In this snippet of the log, a new version of a Host is detected and ActiveMatrix Administrator is updating the Host version to 3.4.0 from 3.3.0HF15.

```

com.tibco.amx.admin.api.host - Detected new version of runtime for host:
SystemHost, starting to sync up node version. old version: 3.3.0.HF15 new
version: 3.4.0
com.tibco.amx.admin.api.host - Admin data update is done for host: SystemHost

```

- In this snippet of the log, a new version of a Host is detected and ActiveMatrix Administrator is updating the Node version to 3.4.0 from 3.3.0HF15.

```

com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Detected new version of runtime for node: DevNode, starting to sync up node
version. old version: 3.3.15 new version: 3.4.0
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Upgrading admin data to sync up with runtime for node : DevNode, from old
version: 3.3.15 to new version: 3.4.0
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Upgrading admin data from 330 to 340 for node:DevNode

```

- In this snippet of the log, ActiveMatrix Administrator is upgrading the Platform Application (and ArtifactServer Application if it is in the ActiveMatrix Administrator Node), deleting REST BT System Applications, and Rest BT System Application Features.

```
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Starting to update Platform (and ArtifactServer) apps to 3.4.0 from 3.3.0.
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Start to
create rest bt component for platform application.
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Rest bt
component doesn't exist in platform application, starting to add it.
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Finished
creating rest bt component for platform application.
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Deleting
application 'com.tibco.amx.bt.rest.application_3.3.0:3.3.0.000' distribution
from node 'DevNode'
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Deleted
application 'com.tibco.amx.bt.rest.application_3.3.0:3.3.0.000' since it has
been removed from all nodes.
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Deleting
enabled feature 'com.tibco.amx.bt.rest.runtime.product.feature' from node
'DevNode'.
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Deleting
runtime feature 'com.tibco.amx.bt.rest.runtime.product.feature' from node
'DevNode'.
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Platform (and ArtifactServer) apps have been updated to 3.4.0.
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Admin data update is done for node: DevNode
```

- In this snippet of the log, ActiveMatrix Administrator is syncing up enabled features on Node.

```
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating admin enabled and runtime feature in Admin DB for node: DevNode
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Syncing runtime and enabled features using HostManager for node: DevNode
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating Enabled Features for node: DevNode
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating version for Feature: com.tibco.gxml.product.feature from version:
1.0.5.000 to version: 3.3.100.000
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating version for Feature: com.tibco.amx.platform.product.feature from
version: 1.3.13.000 to version: 1.3.100.000
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating version for Feature: com.tibco.tibcoxml.product.feature from version:
5.52.0.000 to version: 5.52.100.000
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating version for Feature: com.tibco.amx.it.mediation.product.feature from
version: 3.5.1.000 to version: 3.5.100.000
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Finished Updating Enabled Features for node: DevNode
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating Runtime Features for node: DevNode
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating version for Feature: com.tibco.amx.platform.product.feature from
version: 1.3.13.000 to version: 1.3.100.000
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating version for Feature: com.tibco.gxml.product.feature from version:
1.0.5.000 to version: 3.3.100.000
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating version for Feature: com.tibco.tibcoxml.product.feature from version:
5.52.0.000 to version: 5.52.100.000
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Updating version for Feature: com.tibco.amx.it.mediation.product.feature from
version: 3.5.1.000 to version: 3.5.100.000
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Finished Updating Runtime Features for node: DevNode
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Finished Syncing runtime and enabled features using HostManager for node: DevNode
com.tibco.amf.admin.api.amx.lifecycle.impl.NodeStatusNotificationProcessor -
Finished updating admin enabled and runtime feature in Admin DB for node: DevNode
```



## Downgrading Using TCT Wizard

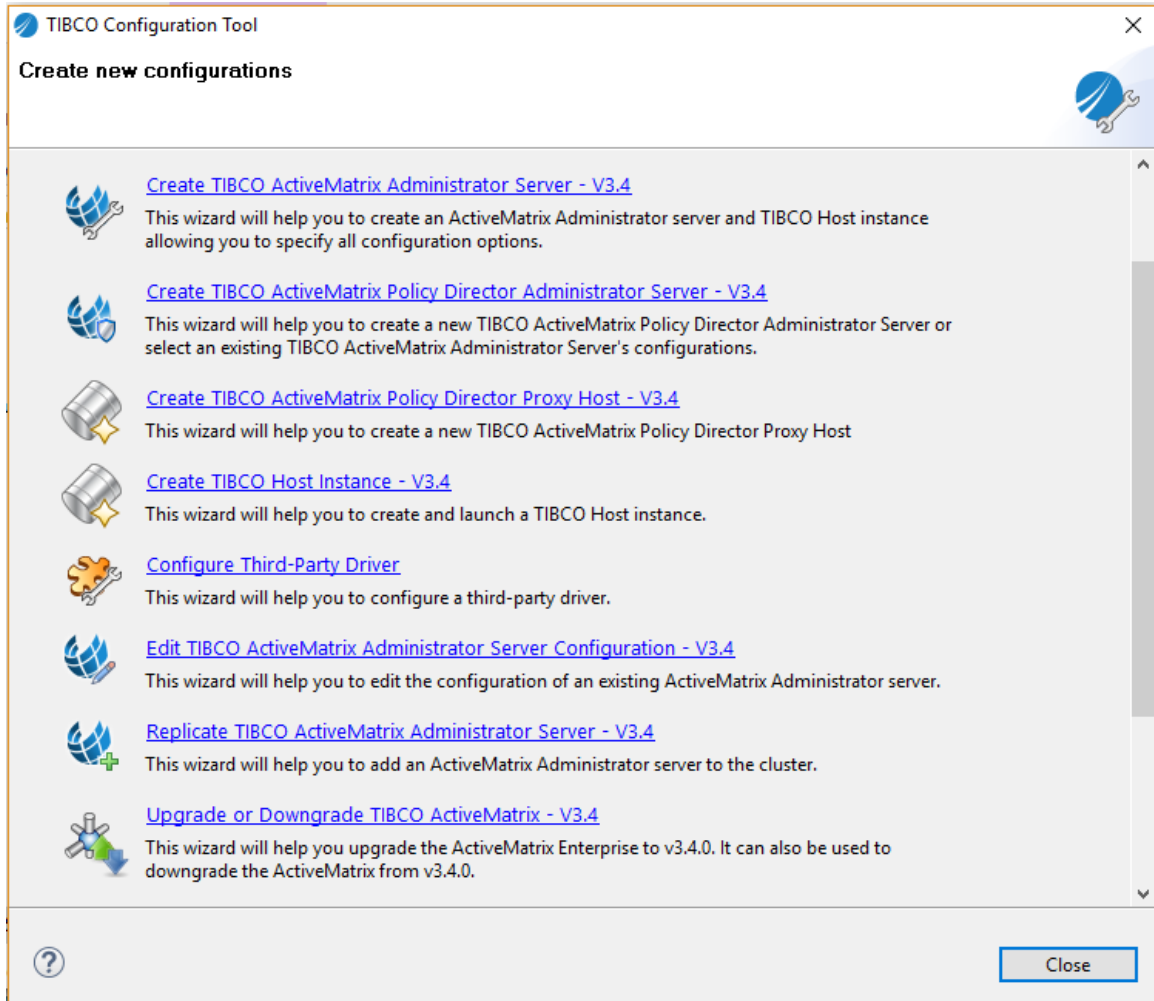
This wizard is similar to the Upgrade wizard in TCT.

### Downgrading Runtime Hosts

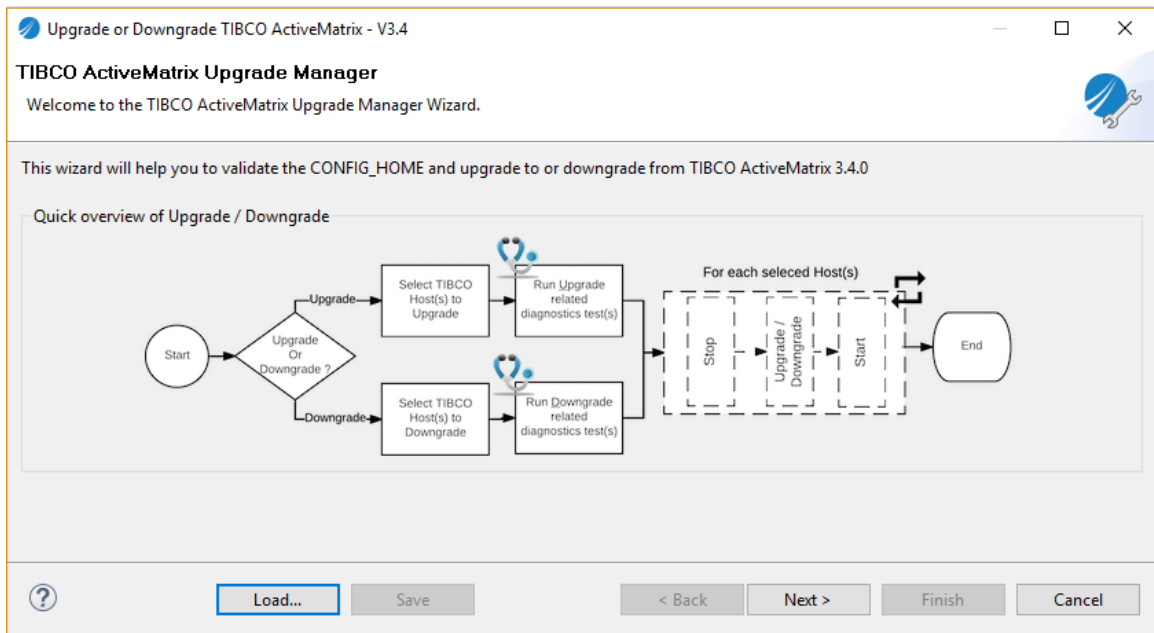
As mentioned earlier, when downgrading, ActiveMatrix Administrator Host or SystemHost must be downgraded *last*. That is, after downgrading all runtime hosts and nodes.

Navigate to `TIBCO_HOME\tct/<version>` and start the TCT wizard by running the `TIBCOConfigurationTool.exe`.

Select the `CONFIG_HOME` to be downgraded. In this case, we select `C:\amx.home\data` and click **OK**.



Click **Upgrade or Downgrade TIBCO ActiveMatrix - V3.4**. The overview workflow of both upgrade and downgrade is displayed.



Click **Next**.

Upgrade or Downgrade TIBCO ActiveMatrix - V3.4

### TIBCO ActiveMatrix Upgrade Manager: Upgrade or Downgrade

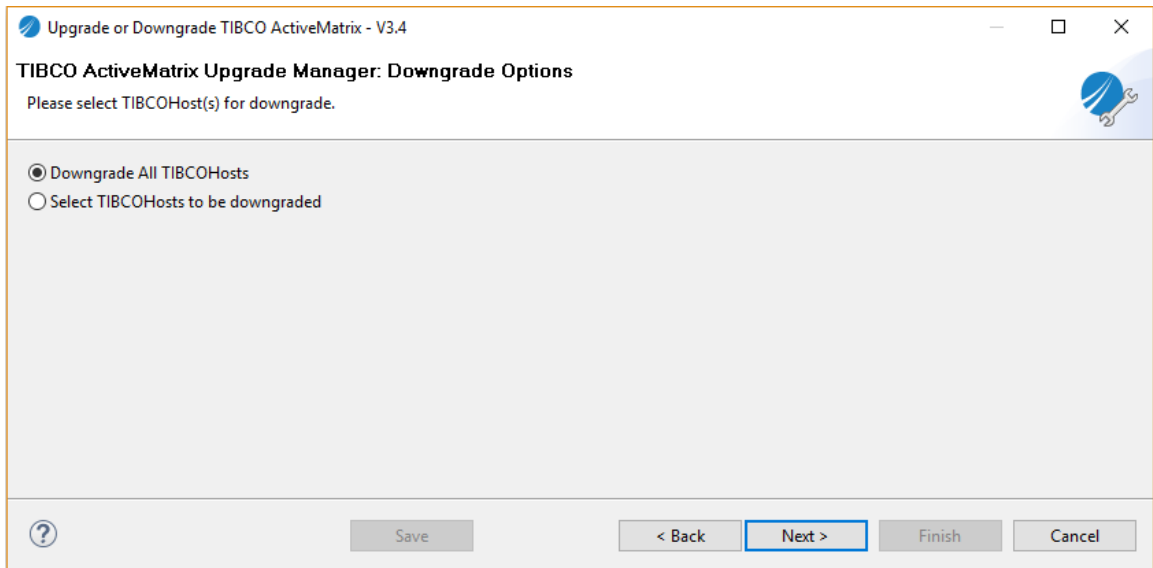
Select upgrade or downgrade.

☐ Upgrade  
This wizard will help you validate the CONFIG\_HOME for a successful upgrade to ActiveMatrix 3.4.0, and then upgrade all or a selection of Hosts to 3.4.0.

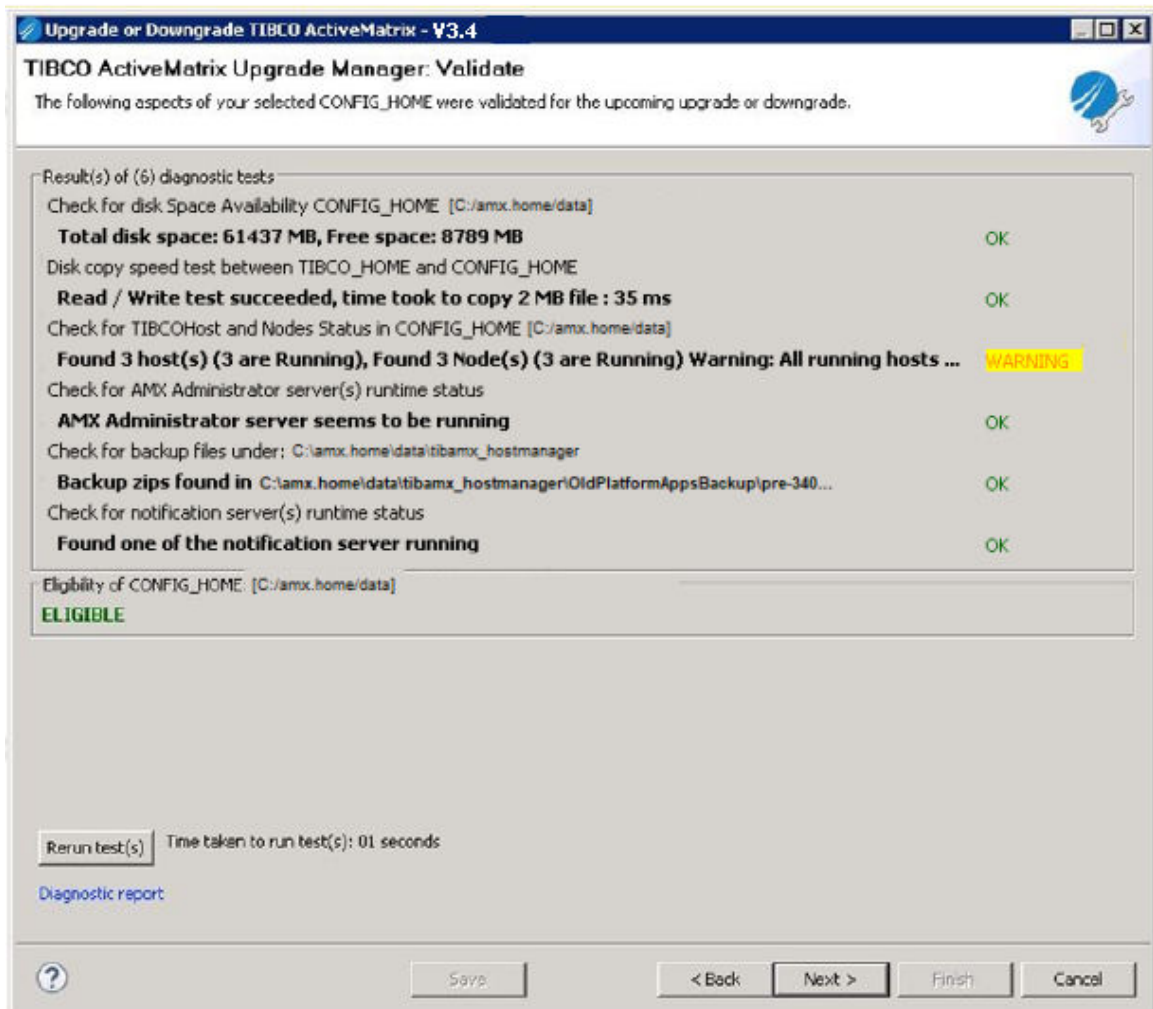
☒ Downgrade  
This wizard will help you validate the CONFIG\_HOME for a successful downgrade from ActiveMatrix 3.4.0, and then downgrade all or a selection of Hosts from 3.4.0.

? Save < Back Next > Finish Cancel

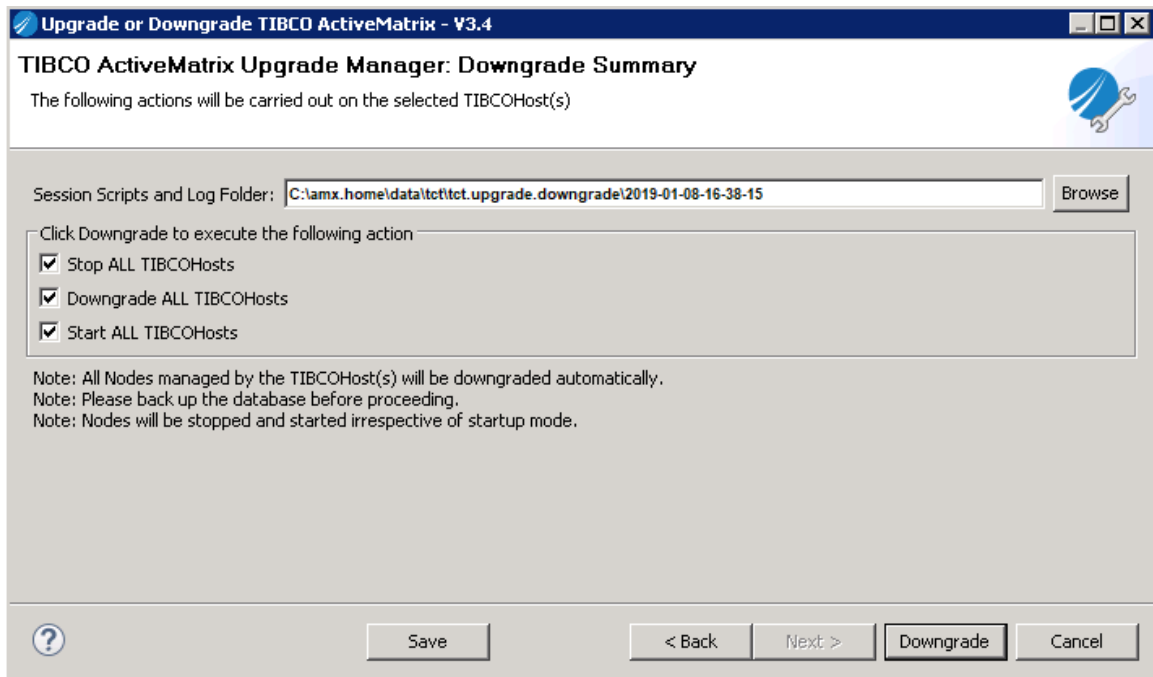
Click **Downgrade**.



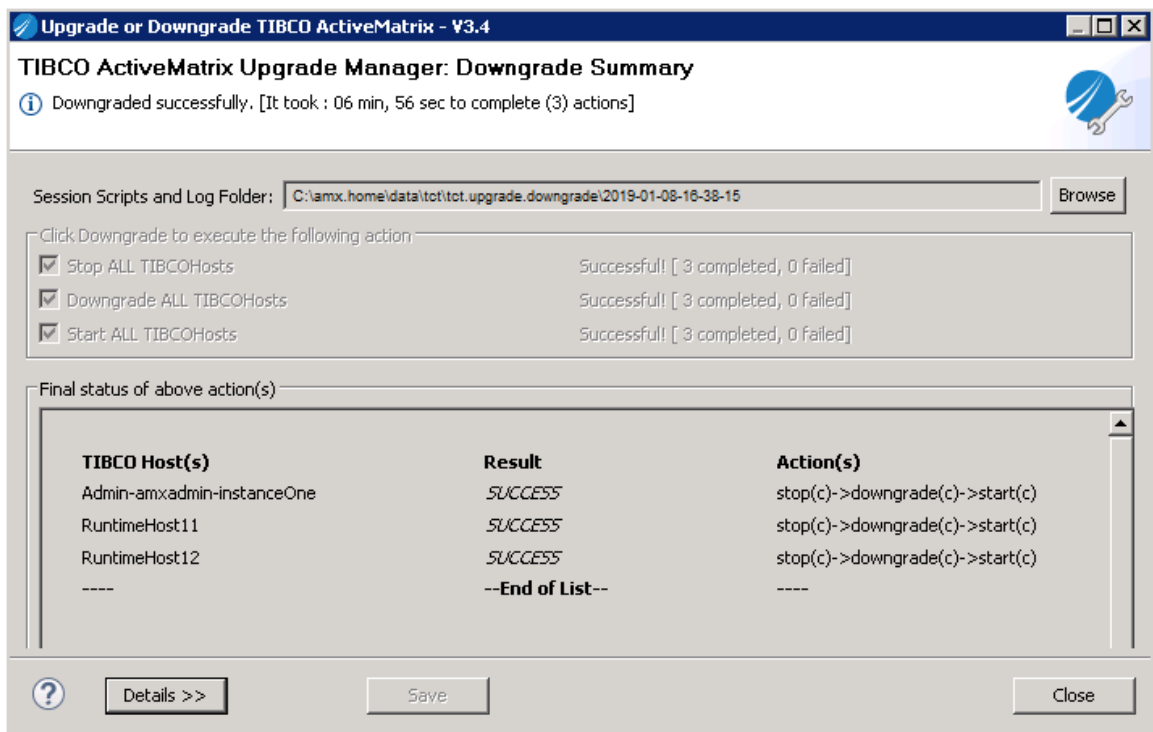
In this example, click **Downgrade All TIBCOHosts**. The following screen shows the aspects of the downgrade that were validated. Click **Next**.



Click **Next**. The following screen lists the actions that are to be executed on a downgrade. It also shows the path of the Session Scripts and Log folder.



Click **Downgrade**. The Downgrade Summary screen is displayed.



### Summary Screen

The Summary screen shows detailed information regarding the Downgrade progress.

The screen shows a table containing the list of Hosts, result of Downgrade and actions with status. When all the actions are completed successfully without any failure, **SUCCESS** is displayed in the **Result** column of the Host. If any action fails, the **Result** column shows **FAILURE**. You can also check the status of each action in the **Action(s)** column, beside the name of the action. One of the following statuses is printed beside the action name:

- Running (r): Action is currently running or being executed
- Completed (c): Action is completed successfully
- Failed (f): Action is completed with failure
- Aborted (a): Action is skipped or aborted

After the downgrade is completed, the total time taken for the downgrade is displayed on the top of the summary screen immediately below the title.

### Downgrading the ActiveMatrix Administrator Instance

Select the CONFIG\_HOME that contains the ActiveMatrix Administrator Server. In this case, it is C:\amx.home\data.

Make sure the Administrator server is in the Running state using the following screen. Enter the configuration details and test the connection.

**Upgrade or Downgrade TIBCO ActiveMatrix - V3.4**

**TIBCO ActiveMatrix Upgrade Manager: Adminsitrator Server**  
Enter configuration details of the Administrator server

Machine Name:

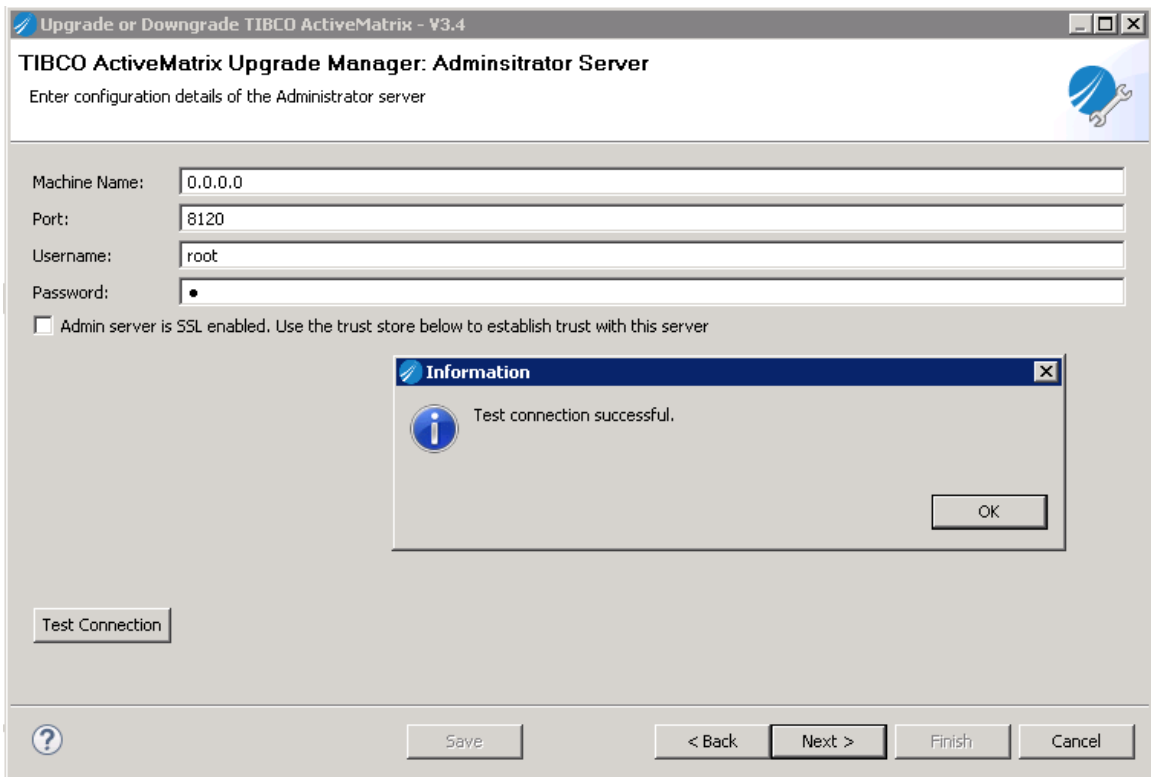
Port:

Username:

Password:

☐ Admin server is SSL enabled. Use the trust store below to establish trust with this server

? Save < Back Next > Finish Cancel



Proceed with the remaining steps. The status of the Downgrade is displayed on the last screen of the wizard. You can take a look at the logs in the folder specified in the **Session Scripts and Log Folders** field.

## Verifying Downgrade

After Downgrading from ActiveMatrix 3.4.0, the following methods can be used to verify whether the Hosts, Nodes, and System Applications are downgraded successfully and to check whether they are using the expected version.



Additional steps are required if REST BT Applications are installed on the Node. These steps are required for the REST BT Application to run smoothly after the Downgrade. It involves bringing back the old REST BT System Application. Refer to [Special Case Scenario on Handling REST BT after a Downgrade](#) for more details.

## Checking Host and Node Version from Administrator UI

After downgrading, all Hosts that are downgraded shows the old version in the **Version** column of the **Infrastructure > Hosts** list. This can be verified by clicking each Host from the Hosts list and checking version in the **General** tab.

Hosts				
Name	Version	Host State	Machine	Action History
SystemHost	3.3.0.HF15	Running	apcVln2k8R2x64-55	<a href="#">Install features successful</a>
RuntimeHost12	3.3.0.HF15	Running	apcVln2k8R2x64-55	<a href="#">Bind Successful</a>
RuntimeHost11	3.3.0.HF15	Running	apcVln2k8R2x64-55	<a href="#">Bind Successful</a>

After downgrading, all the Nodes that are downgraded show the old version in the **Version** column of the **Infrastructure > Nodes** list in Administrator UI.

**Nodes** Environment DevEnvironment

New Delete Install or Sync Uninstall Start Stop

Name	Host	Machine	Node State	Version	Synchronization	Startup Mode	Action History
DevNode	SystemHost	apcWin2k8R2x64-55	Running	3.3.0.HF15	In Sync	Automatic	<a href="#">Change features successful</a>
ProxyNode	SystemHost	apcWin2k8R2x64-55	Running	3.3.0.HF15	In Sync	Automatic	<a href="#">Change features successful</a>

## Checking Host and Node Version from Command Line

Host and Node version can be verified from the command line using the `tibcoHost.exe describeHost` and `tibcoHost.exe describeNodes` command from the `TIBCO_HOME\host\bin` folder.

An example of using `tibcoHost.exe describeHost` command is shown below.

Command:

```
tibcohost.exe describeHost
```

Output:

Invoking `describeHost`

Host description follows:

```
Host name: SystemHost
Enterprise name: amxadmin
HPA instance name: Admin-amxadmin-instanceOne
Bind status: bound
Internet host name: apcWin2k8R2x64-55
HPA type: TibcoHost
HPA specification version: 2.2.0
Host platform version: 3.3.0.HF15
Connect URL: service:jmx:jmxmp://apcWin2k8R2x64-55:6051
O/S name: Windows Server 2008 R2
O/S version: 6.1
O/S process ID: 7968
System architecture: amd64
Secure connection: false
Patch(es) associated with this version:
Upgrade history, current to oldest:
  Host platform version: 3.3.0.HF15, associated patch(es):
amx.platform.patch:3.3.0.HF15
  Host platform version: 3.4.0, associated patch(es): amx.platform.patch:3.4.0
  Host platform version: 3.3.0.HF15, associated patch(es):
amx.platform.patch:3.3.0.HF15
  Host platform version: 3.3.0, no associated patch(es)
Upgrade status: none
```

The Node's version can be found using the `describeNodes` command. An example is shown below.

Command:

```
tibcohost.exe describeNodes
```

Output:

Invoking `describeNodes`

Description of node "DevNode" follows:

```
Node description: Development node
Current status: RUNNING
Node type: com.tibco.amf.hpa.tibcohost.node.hibernate.feature
Node type version: 3.3.15
Platform version: 3.3.0.HF15
Start mode: auto
```

Description of node "ProxyNode" follows:

```
Node description: ProxyNode
Current status: RUNNING
Node type: com.tibco.amf.hpa.tibcohost.node.hibernate.feature
Node type version: 3.3.15
Platform version: 3.3.0.HF15
```

```

Start mode: auto
Description of node "SystemNode" follows:
Node description: Admin Default Node
Current status: RUNNING
Node type: com.tibco.amf.hpa.tibcohost.node.hibernate.feature
Node type version: 3.3.15
Platform version: 3.3.0.HF15
Start mode: auto

```

## Checking Node Logs for Updated Version

After downgrading, when the Node is started, look for the following log lines at the beginning of the Node log. It shows that the Node is running with the older version of TIBCO ActiveMatrix Platform.



These logs may not be available for versions prior to AMX 3.3.0.

Here is an example from the SystemNode.log.

```

com.tibco.amx.hpa.node.Node - %%%%%%%%%%
%%%%%%%%%
com.tibco.amx.hpa.node.Node - TIBCO-AMX-HPA-014681: node "SystemNode" is running
version 3.3.0.HF15 of TIBCO ActiveMatrix Platform
com.tibco.amx.hpa.node.Node - %%%%%%%%%%
%%%%%%%%%

```

## Checking Platform Application Version

After downgrading, the platform application (com.tibco.amx.platform) version is changed to an older version. This can be verified from the Applications Screen of the ActiveMatrix Administrator UI.

Name	Application State	Last Deployed On	Synchronization	Action History
System				
com.tibco.amx.platform (DevNode)	Running	2019-01-08 12:26:27	In Sync	Platform Install Successful
com.tibco.amx.platform (ProxyNode)	Running	2019-01-08 12:29:59	In Sync	Platform Install Successful
com.tibco.amx.it.mediation.apl	Running	2019-01-08 12:30:35	In Sync	Deploy with Start Successful
HelloWorld-1	Running	2019-01-08 12:30:51	In Sync	Deploy with Start Successful

**com.tibco.amx.platform (DevNode)**

**General** | Configuration | Governance | Properties | UDDI Publication | Distribution | Substitution Variables | Resource Templates | Status

**View:** Currently Configured

**Description (optional):** Default platform application [Upgraded from 3.3.0 to 3.4.0 on 01/08/2019 16:08:54] [Downgraded from 3.4.0 to 3.3.0 on 01/08/2019 16:52:16]

**Contact (optional):**

**Application Template Name:** TIBCO ActiveMatrix Platform

**Application Template Version:** 3.3.0.000 [Upload DAA or EAR](#) | [Download DAA](#)

**Application Template Id:** com.tibco.amx.platform.daa

**Modified By:** root

**Modified On:** 2019-01-08 12:26:21

## Analyzing the Downgrade Logs

To help you understand the different stages of the logging process, let us take a look at the Downgrade log samples.

By default, TCT logs are stored in the logs folder under the path mentioned in the **Session Scripts and Logs Folder** in the Summary screen. The entire TCT console logs are available in one file, tct.console.output.TIMESTAMP.log. The logs of each action are tracked in their respective log files. There is a log file for every action. For example, if on a host, there are four actions, there will be four log files corresponding to every action.

The downgrade process generates the following logs:

- Start and stop action logs
- Downgrade action logs



- Downgrade Administrator logs

## Start and Stop Action Logs

Start and stop action logs are simple. On every Host, the output of the start and stop commands is displayed on the console.

## Downgrade Action Logs

Downgrade action logs contain a detailed log of the Downgrade process.

Downgrade logs contain detailed information about the Downgrade process. The [Downgrade](#) section describes all the steps related to the Downgrade process in detail. The following are examples (headers and sample log) from the downgrade logs corresponding to each step in the Downgrade process.

1. **Installing Product Features on a Host:** Product Features of the version that you are downgrading to will be installed on the Host and this can be verified under the following header. For example, the following header shows that it is installing feature of 3.3.0.HF15 version.

```
-----
Installing product features for version : 3.3.0.HF15
-----
```

```
-----
Following product features will be INSTALLED on host
-----
```

2. **Enabling Product Features on Node:** Previous version of the product features are enabled on the Nodes and the corresponding log entries can be found under the following header.

```
-----
Enabling product features on nodes
-----
```

```
-----
Following product features will be ENABLED on node :SystemNode
-----
```

3. **Disabling Product Features:** Corresponding log entries can be found under the following header which contains the list of product features that are disabled on the node.

```
-----
Following product features will be DISABLED on node :SystemNode
-----
```

4. **Uninstalling Product Features:** Product features are uninstalled from the Host after they are disabled from all the Nodes. These logs can be found under the following header.

```
-----
Removing disabled 3.4.0 product features after downgrading host : Admin-amxadmin-
instanceOne
-----
```

```
-----
Following product features will be UNINSTALLED from host
-----
```

5. **Downgrading Wrappers Logs:** To see information on reverting wrappers, look for the following section of the log:

```
Reverting wrappers for the Host instances and Nodes
Updating wrapper for the Host instance: Admin-amxadmin-instanceOne
Successfully updated wrapper for the Host instance: Admin-amxadmin-instanceOne
Updating wrapper for Nodes on Host instance: Admin-amxadmin-instanceOne
Updating wrapper for the Node: DevNode
Successfully updated wrapper for the Node: DevNode
Updating wrapper for the Node: SystemNode
Successfully updated wrapper for the Node: SystemNode
```

6. **Downgrading Platform Application and Putting back REST Binding System Application:** Logs for downgrading platform application (putting back the application from backup) and putting back the add-on REST Binding System Applications can be seen under the following header

```
print-report-start-process:
Doing downgrade
AMX Node(s): [DevNode,SystemNode] found in CONFIG_HOME [C:\amx.home\data
\tibcohost\Admin-amxadmin-instanceOne]
*****
*****
This script will downgrade all node's AMX Platform Application listed below

Total Nodes to process: 2
Node: DevNode
Node: SystemNode

Tibco Home for this AMX Nodes is: C:\tibco
Configuration Home for this AMX Nodes is: C:\amx.home\data\tibcohost\Admin-
amxadmin-instanceOne
Tibcohost name is : Admin-amxadmin-instanceOne
*****
*****
```

7. **Summary:** After the applications are downgraded, it prints a summary of the result as follows:

```
#####
#####
##### Report of platform App downgrade for each node in CONFIG_HOME :
C:\amx.home\data
#####
#####
#Ant properties
#Thu Jul 20 02:39:48 PDT 2017
Admin-amxadmin-instanceOne.node.DevNode=SUCCESS
Admin-amxadmin-instanceOne.node.DevNode.timetaken=18.013 sec
Admin-amxadmin-instanceOne.node.SystemNode=SUCCESS
Admin-amxadmin-instanceOne.node.SystemNode.timetaken=17.303 sec
#####
#####
```

## SystemNode Downgrade Logs

1. Take a look at the following snippet of the log when a new version of a Host is detected and the ActiveMatrix Administrator is updating Host version to 3.3.0.HF15 from 3.4.0.

```
com.tibco.amx.admin.api.host - Detected new version of runtime for host:
SystemHost, starting to sync
up node version. old version: 3.4.0 new version: 3.3.0.HF15
com.tibco.amx.admin.api.host - Admin data update is done for host: SystemHost
```

2. Take a look at the following snippet of the log when a new version of a Host is detected and the ActiveMatrix Administrator is updating the Node version to 3.3.0.HF15 from 3.4.0.

```
com.tibco.amf.admin.api.amx.host.HostService - Detected new version of runtime
for node: SystemNode,
starting to sync up node version. old version: 3.4.0 new version: 3.3.15
com.tibco.amf.admin.api.amx.host.HostService - Upgrading admin data to sync up
with runtime for node : SystemNode,
from old version: 3.4.0 to new version: 3.3.15
com.tibco.amf.admin.api.amx.host.HostService - Downgrading admin data from 340
to 330 for node: SystemNode
```

3. Take a look at the following snippet of the log when the ActiveMatrix Administrator is downgrading a platform Application (and ArtifactServer Application if it is an Administrator Node).

```
com.tibco.amf.admin.api.amx.host.HostService - Starting to update Platform (and
ArtifactServer) apps to 3.3.0 from 3.4.0.
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Start to
remove rest bt component from platform application.
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Finished
```

```

removing rest bt component from platform application.
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Starting
to update Artifact Server application to 3.3.0.000
com.tibco.amf.admin.api.amx.application.impl.ApplicationServiceUtil - Done
updating Artifact Server application to 3.3.0.000
com.tibco.amf.admin.api.amx.host.HostService - Platform (and ArtifactServer)
apps have been updated to 3.3.0.
com.tibco.amf.admin.api.amx.host.HostService - Admin data update is done for
node: SystemNode

```

4. Take a look at the following snippet of the log when the ActiveMatrix Administrator is syncing up enabled Features on Node.

```

com.tibco.amf.admin.api.amx.host.HostService - Updating admin enabled and
runtime feature in Admin DB for node: SystemNode
com.tibco.amf.admin.api.amx.host.HostService - Syncing runtime and enabled
features using NodeProfile for node: SystemNode
com.tibco.amf.admin.api.amx.host.HostService - Updating Enabled Features for
node: SystemNode
com.tibco.amf.admin.api.amx.host.HostService - Updating version for Feature:
com.tibco.tcap.apps.system.apptemplate.rpf
from version: 3.4.100.000 to version: 3.3.13.000
com.tibco.amf.admin.api.amx.host.HostService - Updating version for Feature:
com.tibco.amf.admin.tibcohost.product.feature
from version: 3.4.100.000 to version: 3.3.15.000
com.tibco.amf.admin.api.amx.host.HostService - Updating version for Feature:
com.tibco.amx.platform.product.feature
from version: 1.3.100.000 to version: 1.3.15.000
com.tibco.amf.admin.api.amx.host.HostService - Updating version for Feature:
com.tibco.amx.dashboard.product.feature
from version: 3.4.100.000 to version: 3.3.15.000
com.tibco.amf.admin.api.amx.host.HostService - Finished Updating Enabled
Features for node: SystemNode
com.tibco.amf.admin.api.amx.host.HostService - Updating Runtime Features for
node: SystemNode
com.tibco.amf.admin.api.amx.host.HostService - Updating version for Feature:
com.tibco.amx.platform.product.feature
from version: 1.3.100.000 to version: 1.3.15.000
com.tibco.amf.admin.api.amx.host.HostService - Updating version for Feature:
com.tibco.amf.admin.tibcohost.product.feature
from version: 3.4.100.000 to version: 3.3.15.000
com.tibco.amf.admin.api.amx.host.HostService - Updating version for Feature:
com.tibco.tcap.apps.system.apptemplate.rpf
from version: 3.4.100.000 to version: 3.3.13.000
com.tibco.amf.admin.api.amx.host.HostService - Updating version for Feature:
com.tibco.amx.dashboard.product.feature
from version: 3.4.100.000 to version: 3.3.15.000
com.tibco.amf.admin.api.amx.host.HostService - Finished Updating Runtime
Features for node: SystemNode
com.tibco.amf.admin.api.amx.host.HostService - Finished Syncing runtime and
enabled features using NodeProfile for node: SystemNode
com.tibco.amf.admin.api.amx.host.HostService - Finished updating admin enabled
and runtime feature in Admin DB for node: SystemNode

```

5. Take a look at the following snippet of the log when the ActiveMatrix Administrator is syncing up ActiveMatrix Administrator plugin versions.

```

com.tibco.amf.admin.api.amx.host.HostService - Starting to sync up admin plugin
versions.
com.tibco.amf.admin.api.amx.host.HostService - Finished syncing up admin plugin
versions.

```

6. Take a look at the following snippet of the log when the ActiveMatrix Administrator is creating REST BT System Applications.

```

com.tibco.amx.admin.api.node - Creating REST BT system application for node
'SystemNode'
com.tibco.amx.admin.api.node - Done creating REST BT system application
'com.tibco.amx.bt.rest.application'
for node 'SystemNode'
com.tibco.amx.admin.api.node - Mapping application
'com.tibco.amx.bt.rest.application' to node 'SystemNode'
com.tibco.amx.admin.api.node - Done mapping application

```

```

'com.tibco.amx.bt.rest.application' to node 'SystemNode'
com.tibco.amx.admin.api.node - Creating REST BT system application for node
'SystemNode'
com.tibco.amx.admin.api.node - Done creating REST BT system application
'com.tibco.amx.bt.rest.application.admin'
for node 'SystemNode'
com.tibco.amx.admin.api.node - Mapping application
'com.tibco.amx.bt.rest.application.admin' to node 'SystemNode'
com.tibco.amx.admin.api.node - Done mapping application
'com.tibco.amx.bt.rest.application.admin' to node 'SystemNode'

```

- Take a look at the following snippet of the log when the ActiveMatrix Administrator is marking Applications which have REST BT as out of sync.

```

com.tibco.amx.admin.api.node - Marking application 'rest-java_1' as 'out of
sync' for node 'SystemNode'
com.tibco.amx.admin.api.node - Done marking application 'rest-java_1' as 'out of
sync' for node 'SystemNode'

```

### Special Case Scenario on Handling REST BT after a Downgrade

After downgrading to ActiveMatrix 3.3.0 or ActiveMatrix 3.2.0, the newly created REST BT System Applications are Out of Sync and in the Not deployed State.

#### Applications

New  Delete  Deploy  Undeploy  Start  Stop  Move					
Name	Application State	Last Deployed On	Synchronization	Action History	
System					
amx.platform.apps					
com.tibco.amx.platform (SystemNode)	Running	2017-02-21 04:10:34	In Sync	<a href="#">Start Successful</a>	
com.tibco.amx.platform.artifactserver	Running	2017-02-21 04:12:47	In Sync	<a href="#">Deploy with Start Successful</a>	
com.tibco.amx.platform.dashboard	Running	2017-02-21 04:12:59	In Sync	<a href="#">Deploy with Start Successful</a>	
com.tibco.amx.bt.rest.application_3.3.0_1	Not Deployed		Out of Sync		
com.tibco.amx.bt.rest.application.admin_3.3.0	Not Deployed		Out of Sync		

All REST user Applications are in the Partially Deployed state.

#### Applications

New  Delete  Deploy  Undeploy  Start  Stop  Move					
Name	Application State	Last Deployed On	Synchronization	Action History	
System					
amx.platform.apps					
com.tibco.amx.platform (DevNode)	Running	2017-02-21 04:35:14	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.platform (DevNodeHost1No	Running	2017-02-21 04:35:24	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.platform (DevNodeHost1No	Running	2017-02-21 04:36:22	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.platform (DevNodeHost2No	Running	2017-02-21 04:37:02	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.platform (DevNodeHost2No	Running	2017-02-21 04:38:03	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.it.mediation.appt	Running	2017-02-21 05:39:44	In Sync	<a href="#">Deploy with Start Successful</a>	
com.tibco.amx.bt.rest.application_3.3.0	Running	2017-07-20 16:26:46	Out of Sync	<a href="#">Deploy with Start Successful</a>	
jv.helloworld1.soa	Running	2017-02-21 05:39:51	In Sync	<a href="#">Deploy with Start Successful</a>	
mediation.helloworld.log	Running	2017-02-21 05:39:44	In Sync	<a href="#">Deploy with Start Successful</a>	
rest-java	Partially deployed	2017-07-20 16:27:07	Out of Sync	<a href="#">Deploy with Start Successful</a>	

Perform the following post-downgrade steps to bring the user Applications back to Running and In sync states.

### Procedure

- Uninstall ActiveMatrix 3.4.0. If you do not uninstall the product, the deployment of REST BT user Application will fail because ActiveMatrix Administrator will try to provision the 3.4.0 platform product feature. Perform the steps under [Uninstalling TIBCO ActiveMatrix Service Grid in the GUI Mode](#).

2. Deploy all REST BT System Applications. Perform the steps mentioned in [Deploying REST BT System and User Applications](#).
3. Restart all nodes which have the REST BT user Applications.
4. Deploy REST BT user Applications.

### Uninstalling TIBCO ActiveMatrix Service Grid in the GUI Mode

Uninstall ActiveMatrix 3.4.0. If you do not uninstall the product, the deployment of REST BT user Application will fail because ActiveMatrix Administrator will try to provision the 3.4.0 platform product feature.

#### Procedure

1. Navigate to `TIBCO_HOME\tools\universal_installer\TIBCOUniversalInstaller-x86-64.exe`.
2. Select **Uninstall Products from a TIBCO\_HOME Location**.
3. Specify a **TIBCO\_HOME Location** and click **Next**.
4. Select **Custom Uninstall (select the products to be removed)** and click **Next**.
5. From the **Products Available for Uninstall** list, select **TIBCO ActiveMatrix Service Grid 3.4.0**.
6. Click **Uninstall**. A summary of the uninstallation is displayed.
7. Click **Finish**.
8. Restart the ActiveMatrix Administrator and all other instances.

#### What to do next

Perform the steps mentioned in [Deploying REST BT System and User Applications](#).

### Deploying REST BT System and User Applications

#### Prerequisites

Perform the steps mentioned in [Uninstalling TIBCO ActiveMatrix Service Grid in the GUI Mode](#).

#### Procedure

1. Navigate to the System Environment and deploy the REST BT System Application.
2. Restart the Node on which the REST BT user Applications are deployed.
3. Deploy all REST BT user Applications.
4. Check if all the REST BT user Applications are in the Running state.

## Applications

New ▼  Delete ▼  Deploy ▼  Undeploy ▼  Start  Stop ▼  Move					
Name ▲	Application State	Last Deployed On	Synchronization	Action History	
System					
amx.platform.apps					
com.tibco.amx.platform (DevNode)	Running	2017-02-21 04:35:14	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.platform (DevNodeHost1Node1)	Running	2017-02-21 04:35:24	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.platform (DevNodeHost1Node2)	Running	2017-02-21 04:36:22	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.platform (DevNodeHost2Node3)	Running	2017-02-21 04:37:02	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.platform (DevNodeHost2Node4)	Running	2017-02-21 04:38:03	In Sync	<a href="#">Platform Install Successful</a>	
com.tibco.amx.bt.rest.application_3.3.0	Running	2017-04-18 11:16:37	In Sync	<a href="#">Deploy with Start Successful</a>	
com.tibco.amx.it.mediation.apt	Running	2017-02-21 05:39:44	In Sync	<a href="#">Deploy with Start Successful</a>	
com.tibco.amx.bt.rest.application	Running	2017-04-18 12:08:51	In Sync	<a href="#">Deploy with Start Successful</a>	
jv.helloworld1.soa	Running	2017-02-21 05:39:51	In Sync	<a href="#">Deploy with Start Successful</a>	
mediation.helloworld.log	Running	2017-02-21 05:39:44	In Sync	<a href="#">Deploy with Start Successful</a>	
rest-java	Running	2017-04-18 12:09:29	In Sync	<a href="#">Deploy with Start Successful</a>	

## Result

If the REST BT user Applications are in the Running state, the Downgrade was successful.

# Host Manager

Host Manager is a Command Line (CLI) tool that can be used to apply or revert a software patch or Engineering Build. The tool contains other commands to carry out various actions in the ActiveMatrix Installation, and are explained in subsequent sections in detail.



Host Manager Tool replaces the Patch Manager Tool that was available in the earlier version of ActiveMatrix.

## Running the Host Manager Tool

Run `TIBCO_HOME\amx\<version>\bin\tibamx_hostmanager.exe`.



All commands demonstrated below are assumed to be running from the interactive shell.

## Help

To get information on the supported commands, run the following:

```
>help
```

To get detailed information on the usage of a specific command and its supported arguments, run the following:

```
>help <COMMAND_NAME>
```



<TIBCO\_HOME> in this section refers to the TIBCO Home from where the Host Manager is running.  
<CONFIG\_HOME> refers to the directory where you created or configured the Enterprise which contains Hosts and Nodes using TIBCO Configuration Tool (TCT).

## Patch Commands

ActiveMatrix hotfixes are installed on the TIBCO\_HOME using the TIBCO Universal Installer. One or more patches get installed when a hotfix is installed. These patches are then applied to the existing configuration (Hosts and Nodes in the CONFIG\_HOME).

The following patch commands are available:

Command	Description
describeAvailablePatches	Provides the list of patches that are installed and are available to be applied to TIBCO Host instances.
describeAppliedPatches	Provides the list of patches that are applied to a particular TIBCO Host instance.
applyPatch	Applies a Patch to TIBCO Host instances.
revertPatch	Reverts a Patch applied to TIBCO Host instances.

## describeAvailablePatches

The "describeAvailablePatches" command provides information about all patches currently installed at the specified install location and available for applying to TIBCO Host instances.

## Arguments

See [Common Arguments](#).

## Example

```
> describeAvailablePatches
```

## describeAppliedPatches

The "describeAppliedPatches" command provides information about all patches that have been applied to the specified TIBCO Host instance.

### Arguments

See [Common Arguments](#).

### Examples

```
> describeAppliedPatches -adminServerDir path/to/CONFIG_HOME/location -ID  
amx.platform.patch:3.3.0.HF17  
  
> describeAppliedPatches -configHomeLocation path/to/CONFIG_HOME/location -  
instanceName my-instance
```

## applyPatch

The "applyPatch" command applies a patch to a TIBCO Host instance or to all TIBCO Host instances in CONFIG\_HOME.

Some patches are successive in nature, and may require other patches to be applied before the new patch can be applied. The "describeAvailablePatches" command will tell you which patches require other patches to be applied first.

Applying a patch consists of two operations, and they are executed depending on the scope of the patch.



- The first operation upgrades the TIBCO Host itself.
- The second operation upgrades the software running in all the Nodes of TIBCO Host. If a patch does not affect the TIBCO Host, the TIBCO Host is not modified. Similarly, if a patch does not affect Node software, Nodes will not be modified. If any errors are encountered during application of a patch, all changes are rolled back and the TIBCO Host instance is not modified.



The TIBCO Host instance must not be in the Running state, at the time of applying the patch. All Nodes managed by the instance must be stopped first before applying the patch.

Argument	Description
-ID	The identifier of the patch to be applied. Identifiers are of the form <name>:<version>.  You can get a list of available Patch IDs using the "describeAvailablePatches" command.
-handleStop	Stops TIBCOHost instance(s) before applying the patch.
-handleStart	Starts TIBCOHost instance(s) with "clearCache" after applying the patch. Starts TIBCOHost instance as a Service if it is installed as Windows Service.



Argument	Description
<code>-nonInteractive</code>	<p>Automatically applies the last-released patch from TIBCO_HOME to all TIBCO Host instances in the provided CONFIG_HOME, without any interaction from the user.</p> <ul style="list-style-type: none"> <li>For all TIBCO ActiveMatrix patches, the last-released patch is the last element in the sorted list returned by the "describeAvailablePatches" command.</li> <li>If there are other patches (for example, REST BT, BusinessWorks SE, and so on), the patch with a later release date is applied. For example, if REST BT HotFix 002 was released BEFORE ActiveMatrix HotFix 014 and both are installed at the same time, the Host Manager applies ActiveMatrix HotFix 014, as it was the last one to be released.</li> </ul>
<code>-clearCache</code>	<p>Clear the cache of all participating nodes without starting the TIBCOHost instance on which the nodes are running.</p> <div data-bbox="651 787 1476 945">  <p>If you intend to start Host instances manually, ensure that ALL Hosts are started with "clearCache". Alternatively, use "-clearCache" while running this command. TIBCOHost instances will start with "clearCache" on their next startup.</p> </div> <p>With this, the TIBCOHost instances started from outside of ActiveMatrix (for example, using TIBCO Hawk<sup>®</sup>) after applying the patch can automatically be started with "clearCache" without providing an additional argument. The "clearCache" argument can also be used to start TIBCOHost instances running as Windows Service with "clearCache". You must specify the "clearCache" when applying a patch on TIBCOHost Instance(s) running as Windows Service.</p> <div data-bbox="651 1228 1476 1396">  <p>This command does not handle "clearCache" start of Hosts running as NT Service by default. This can be handled by "-clearCache". If you have Hosts running as NT Service, you must specify "-clearCache" along with "-handleStart" to start the Hosts with "clearCache".</p> </div>
<code>-delayInSeconds</code>	<p>Allows adding a delay of specified amount of time after applying the patch and between each TIBCO Host instance startup if TIBCOHost startup is handled. If the delay is not provided, it uses the default delay of 10 seconds.</p>
<code>-dryRun</code>	<p>Allows you to see what changes would be made by applying a patch, without making the actual changes. The command executes without making changes and you can look in the log to see what changes would have been made.</p>

### Examples

```
>applyPatch -configHomeLocation /path/to/confighome/location -instanceName
myTibcoHostInstance -ID amx.platform.patch:3.3.0.HF14 -handleStop -handleStart
```

This stops the TIBCOHost Instance `myTibcoHostInstance` in the `CONFIG_HOME path/to/confighome/location`, applies the patch `amx.platform.patch:3.3.0.HF14` and starts the Instance with "`clearCache`".



By default, this starts TIBCOHosts running as Windows Service without the "`clearCache`" option.

```
>applyPatch -configHomeLocation /path/to/confighome/location -nonInteractive
```

This applies the latest available patch in `TIBCO_HOME` to *all* TIBCOHost Instances in the `CONFIG_HOME path/to/confighome/location`.

```
>applyPatch -configHomeLocation /path/to/confighome/location -instanceName myTibcoHostInstance -ID amx.platform.patch:3.3.0.HF14 -clearCache
```

This applies the patch `amx.platform.patch:3.3.0.HF14` to TIBCOHost Instance `myTibcoHostInstance` in the `CONFIG_HOME path/to/confighome/location` and clears cache of all Nodes on the Instance `myTibcoHostInstance`.

```
>applyPatch -configHomeLocation /path/to/confighome/location -clearCache
```

This applies the latest available patch in `TIBCO_HOME` to *all* TIBCOHost Instances in the `CONFIG_HOME path/to/confighome/location` and clears cache of *all* Nodes on *all* TIBCOHost Instances.

```
>applyPatch -configHomeLocation /path/to/confighome/location -handleStop -handleStart -clearCache
```

This stops *all* TIBCOHost Instances in the `CONFIG_HOME path/to/confighome/location`, applies the latest available patch to all of them, clears cache of *all* Nodes on *all* of the TIBCOHost Instances and starts the Instances. This starts all Instances with "`clearCache`" whether they are running as processes or as Windows Service.

```
>applyPatch -configHomeLocation /path/to/confighome/location -handleStop -handleStart -delayInSeconds 30
```

This stops all TIBCOHost Instances in the `CONFIG_HOME path/to/confighome/location`, applies the latest available patch to all of them and starts the Instances with "`clearCache`". This adds a delay of 30 seconds after applying the patch and between each TIBCOHost instance startup.

## revertPatch

The "`revertPatch`" command reverts an existing patch from a TIBCO Host instance or from all TIBCO Host instances in a `CONFIG_HOME`.


This command reverts the specified patch as well as all patches with the same ID and a later version. This behavior is useful if you apply several patches of different version at once and want to revert all of them with a single command. You simply revert the oldest of the group of patches, and all the newer ones will be reverted at the same time.

If the patch being reverted is not the most recently applied patch, all patches between the most recently applied and that requested (inclusive) are automatically reverted.



The TIBCO Host instance must not be in Running state. All Nodes managed by the instance must be stopped first to revert a patch.

Argument	Description
-ID	The identifier of the patch to be reverted. Identifiers are of the form <code>&lt;name&gt;:&lt;version&gt;</code> . You can get a list of applied Patch IDs with the " <code>describeAppliedPatches</code> " command.
-handleStop	Stops TIBCOHost instance(s) before reverting the patch.
-handleStart	Starts TIBCOHost instance(s) with " <code>clearCache</code> " after reverting the patch. Starts TIBCOHost instance as a Service if it is installed as Windows Service.

Argument	Description
-clearCache	<p>Clears the cache of all participating Nodes without starting the TIBCOHost Instance on which the Nodes are running.</p> <p>The "clearCache" argument can also be used to start TIBCOHosts running as Windows Service with "clearCache". You must specify the "clearCache" when reverting a patch from TIBCOHost Instance(s) running as Windows Service.</p> <div>  <ul style="list-style-type: none"> <li>If you intend to start Host instances manually, ensure that ALL Hosts are started with "clearCache". Alternatively, use the "-clearCache" argument while running this command. This clears cache of all Nodes on Host instance(s) after reverting the patch without starting them.</li> <li>This command does not handle "clearCache" start of Hosts running as NT Service by default. This can be also be handled by "-clearCache" flag. If you have Hosts running as NT Service, you must specify "-clearCache" along with "-handleStart" to start the Hosts with "clearCache".</li> </ul> </div>
-delayInSeconds	Delay after reverting the patch and between each TIBCO Host instance startup. This argument is optional. The command will use the default delay of 10 seconds.
-nonInteractive	Run in non-interactive mode.
-dryRun	Allows you to see what changes would be made by reverting a patch, without making the actual changes. The command executes without making changes and you can look in the log to see what changes would have been made.

## Examples

```
>revertPatch -configHomeLocation /path/to/confighome/location -instanceName myTibcoHostInstance -ID amx.platform.patch:3.3.0.HF14 -handleStop -handleStart
```

This stops the TIBCOHost Instance myTibcoHostInstance in the CONFIG\_HOME path/to/confighome/location, reverts the patch amx.platform.patch:3.3.0.HF14, and starts the Instance with "clearCache".



By default, this starts TIBCOHosts running as Windows Service without the "clearCache" option.

```
>revertPatch -configHomeLocation /path/to/confighome/location -instanceName myTibcoHostInstance -ID amx.platform.patch:3.3.0.HF14 -clearCache
```

This reverts the patch amx.platform.patch:3.3.0.HF14 from TIBCOHost Instance myTibcoHostInstance in the CONFIG\_HOME path/to/confighome/location and clears cache of all Nodes on the Instance myTibcoHostInstance.

```
>revertPatch -configHomeLocation /path/to/confighome/location -instanceName myTibcoHostInstance -ID amx.platform.patch:3.3.0.HF14 -handleStop -handleStart -clearCache
```

This stops the TIBCOHost Instance myTibcoHostInstance in the CONFIG\_HOME path/to/confighome/location, reverts the patch amx.platform.patch:3.3.0.HF14, clears cache of all Nodes on the Instance and starts the Instance. This starts the Instance with "clearCache" whether it is running as a process or as a Windows Service.

## Engineering Build Commands

The Host Manager provides commands to simplify the process of applying and reverting an Engineering Build in Enterprises with a large number of TIBCOHost Instances.

An Engineering Build, or "EB", is an interim build consisting of one or more defect fixes, intended to be used on a product release which has been made available (GA) to all customers. The purpose of an Engineering Build could be:

1. to diagnose or identify the source of the problem in a particular release; or
2. to confirm whether a certain solution for the customer's problem works as expected, without, or prior to, providing the solution as part of a general release.

Engineering Builds are usually provided to customers to be used in test environment, and typically, depending on the issue in question, may have to be applied individually to many or all the Nodes in the Enterprise.

### applyEB




The "applyEB" command applies a given Engineering Build (EB) to TIBCO\_HOME and to the specified TIBCOHost Instance in the CONFIG\_HOME. If Instance name is not provided, it applies the Engineering Build to all TIBCOHost Instances in a provided CONFIG\_HOME. By default, it stops all TIBCOHost Instances before applying the Engineering Build and after successful application of the Engineering Build, it starts all TIBCOHost Instances with "clearCache". If a TIBCOHost Instance is installed as Windows Service, this command starts the Instance as a Service. Before applying the Engineering Build, it takes a backup of the existing files into <CONFIG\_HOME>/EngineeringBuilds/Before\_<nameOfEBZip>\_backup/ folder where "nameOfEBZip" is the name of the Engineering Build zip file (for example, "TIB\_amx\_<version>\_engineering\_build<buildNumber>"). It also copies the readme file for the specified Engineering Build to <TIBCO\_HOME>/\_ebInstallInfo folder.

This command identifies whether the Engineering Build is targeted for ActiveMatrix Hawk microagent. If the Engineering Build is targeted for ActiveMatrix Hawk microagent, the command applies the Engineering Build to the given ActiveMatrix Hawk microagent and to TIBCO Home. In such case, the Engineering Build is not applied to the CONFIG\_HOME.

- The TIBCO Host instances must not be running and all nodes on the instances must be stopped to apply an Engineering Build. If you have other CONFIG\_HOME running from same TIBCO\_HOME, all Host instances on those CONFIG\_HOME must be stopped manually before applying an Engineering Build. This command will stop Host instances from the given CONFIG\_HOME only.
- After applying the Engineering Build, the command copies the readme file released with the Engineering Build (for example, TIB\_amx\_<version>\_engineering\_build<buildNumber>\_readme.txt for Engineering Build TIB\_amx\_<version>\_engineering\_build<buildNumber>) to <TIBCO\_HOME>/\_ebInstallInfo folder.
- This command applies the JAR files from the specified Engineering Build into appropriate location(s). However, there might be additional actions required to enable this Engineering Build, that is, updating TRA properties and so on. Refer to the readme file released with the Engineering Build (for example, TIB\_amx\_<version>\_engineering\_build<buildNumber>\_readme.txt for Engineering Build TIB\_amx\_<version>\_engineering\_build<buildNumber>) to ensure that all of the required steps are carried out.



## Arguments

Argument	Description
-configHomeLocation	The location of the CONFIG_HOME.
-instanceName	Name of TIBCO Host instance. This argument is optional; It will apply EB to all TIBCO Host instances in the CONFIG_HOME, if not provided.
-ebLocation	The location of the Engineering Build file.
-hawkLibLocation	The location of ActiveMatrix Hawk microagent's 'lib' folder. For example, HAWK_HOME/hawk/<version>/lib. This argument is required if the Engineering Build is targeted for ActiveMatrix Hawk microagent.
-skipStop	Does not stop TIBCOHost instance(s) before applying the Engineering Build.   If you are using this argument, ensure that ALL the Hosts in the given CONFIG_HOME are shutdown completely before calling this command as it could cause severe errors if it is not the case. This command does not verify that the Hosts are shutdown.
-skipStart	Does not start TIBCOHost instance(s) after applying the Engineering Build.   If you are using this argument and intend to start Host instances manually, ensure that ALL Hosts are started with "clearCache". Alternatively, you can use "-clearCache" when running this command. This clears cache of all Nodes on all Host instances after applying the Engineering Build without starting them.
-nonInteractive	Runs in non-interactive manner. No interaction is required from the user during command execution.
-clearCache	Clear the cache without starting TIBCOHost instance(s).   If you have Hosts running as NT Service, you must specify "-clearCache" flag in order to start the Hosts with "clearCache".
-delayInSeconds	Adds delay after applying the Engineering Build and between each TIBCO Host instance startup.

## Examples

```
>applyEB -configHomeLocation /path/to/confighome/location -instanceName
myTibcoHostInstance -ebLocation /path/to/TIB_amx_3.x.x_engineering_build085.zip
```

This stops TIBCOHost Instance myTibcoHostInstance in the CONFIG\_HOME path/to/confighome/location, applies the Engineering Build TIB\_amx\_3.x.x\_engineering\_build085.zip to TIBCO\_HOME and to the Instance myTibcoHostInstance and starts the Instance with "clearCache".

```
>applyEB -configHomeLocation /path/to/confighome/location -ebLocation /path/to/TIB_amx_3.x.x_engineering_build085.zip
```

This stops *all* TIBCOHost Instances in the CONFIG\_HOME path/to/confighome/location, applies the Engineering Build TIB\_amx\_3.x.x\_engineering\_build085.zip to TIBCO\_HOME and to all of the Instances and starts the Instances with "clearCache".

```
>applyEB -configHomeLocation /path/to/confighome/location -ebLocation /path/to/TIB_amx_3.x.x_engineering_build085.zip -skipStop -skipStart
```

This skips the step to stop TIBCOHost instance(s) and applies the Engineering Build TIB\_amx\_3.x.x\_engineering\_build085.zip to TIBCO\_HOME and to all of the Instances in the CONFIG\_HOME /path/to/confighome/location. It skips the step to start TIBCOHost instance(s).

## revertEB

The "revertEB" command reverts an Engineering Build from TIBCO\_HOME and from the given TIBCOHost Instance in the CONFIG\_HOME. If Instance name is not provided, it reverts the Engineering Build from all TIBCOHost Instances in a provided CONFIG\_HOME. To revert an Engineering Build, the user needs to specify the location of the backup folder created by "applyEB" command for that Engineering Build inside <CONFIG\_HOME>/EngineeringBuilds folder. By default, it stops all TIBCOHost Instances before reverting the Engineering Build and after successfully reverting the Engineering Build, it starts all TIBCOHost Instances with "clearCache". If a TIBCOHost Instance is installed as Windows Service, this command starts the Instance as a Service.

This command identifies whether the Engineering Build to be reverted is for ActiveMatrix Hawk microagent. If the Engineering Build is for ActiveMatrix Hawk microagent, it will revert the Engineering Build from TIBCO\_HOME only and the revert from ActiveMatrix Hawk microagent must be handled manually. In such case, the Engineering Build does not need to be reverted from the CONFIG\_HOME.






The TIBCO Host instances must not be running and all nodes on the instances must be stopped to revert an Engineering Build. If you have other CONFIG\_HOME running from same TIBCO\_HOME, all Host instances on those CONFIG\_HOME must be stopped manually before reverting an Engineering Build. This command will stop Host instances from the given CONFIG\_HOME only.

## Arguments

Argument	Description
-configHomeLocation	The location of CONFIG_HOME.
-instanceName	Name of TIBCO Host instance. This argument is optional; It will revert EB from all TIBCO Host instances in the <CONFIG_HOME>.
-ebBackupLocation	The location of the Engineering Build backup folder inside <CONFIG_HOME>/EngineeringBuilds/. This is the location where the original bundles were copied before applying the Engineering Build.



Argument	Description
-skipStop	<p>Skip automated stopping of TIBCO Host instances before reverting the Engineering Build. This argument is optional.</p> <p> If you are using "-skipStop" argument, ensure that the Hosts are shutdown completely before calling this command as it could cause severe errors if it is not the case. This command does not verify that the Hosts are shutdown.</p>
-skipStart	<p>Skip automated starting of TIBCO Host instances after reverting the Engineering Build. This argument is optional.</p> <p> If you are using "-skipStart" argument and intend to start Host instances manually, ensure that ALL Hosts are started with "clearCache". Alternatively, you can use a flag "-clearCache" when running this command. This clears cache of all Nodes on all Host instances after reverting the Engineering Build without starting them.</p>
-clearCache	<p>Clear the cache of ALL nodes on ALL TIBCO Host instances without starting them. This argument is optional.</p> <p> This command does not handle "clearCache" start of Hosts running as NT Service by default. This can be also be handled by "-clearCache" flag. If you have Hosts running as NT Service, you must specify "-clearCache" flag in order to start the Hosts with "clearCache".</p>
-delayInSeconds	<p>Delay after reverting Engineering Build and between each TIBCO Host instance startup. This argument is optional. The command will use the default delay of 10 seconds.</p>
-nonInteractive	<p>Runs in non-interactive manner. No interaction is required from the user during command execution.</p>

## Examples

```
>revertEB -configHomeLocation /path/to/confighome/location -instanceName
myTibcoHostInstance -ebBackupLocation /path/to/confighome/EngineeringBuilds/Before_
TIB_amx_3.x.x_engineering_build085_backup
```

This stops the TIBCOHost Instance myTibcoHostInstance in the CONFIG\_HOME /path/to/confighome/location, reverts Engineering Build TIB\_amx\_3.x.x\_engineering\_build085 from TIBCO\_HOME and from the Instance myTibcoHostInstance using the backup folder at /path/to/confighome/EngineeringBuilds/Before\_ TIB\_amx\_3.x.x\_engineering\_build085\_backup and starts the Instance with "clearCache".

```
>revertEB -configHomeLocation /path/to/confighome/location -ebBackupLocation /
path/to/confighome/EngineeringBuilds/Before_
TIB_amx_3.x.x_engineering_build085_backup
```

This stops *all* TIBCOHost Instances in the CONFIG\_HOME /path/to/confighome/location, reverts Engineering Build TIB\_amx\_3.x.x\_engineering\_build085 from TIBCO\_HOME and from all of the


Instances using the backup folder at /path/to/confighome/EngineeringBuilds/Before\_TIB\_amx\_3.x.x\_engineering\_build085\_backup and starts the Instances with "clearCache".

```
>revertEB -configHomeLocation /path/to/confighome/location -ebBackupLocation /
path/to/confighome/EngineeringBuilds/Before_
TIB_amx_3.x.x_engineering_build085_backup -skipStop -skipStart
```

This skips the step to stop TIBCOHost instance(s) and reverts Engineering Build TIB\_amx\_3.x.x\_engineering\_build085 from TIBCO\_HOME and from all of the Instances in the CONFIG\_HOME /path/to/confighome/location using the backup folder at /path/to/confighome/EngineeringBuilds/Before\_TIB\_amx\_3.x.x\_engineering\_build085\_backup. It skips the step to start TIBCOHost instance(s).

## Host and Node Commands

This section describes commands related to Hosts and Nodes. The commands available are:

Command	Description
startAllHosts	Starts all TIBCOHost Instances in the specified CONFIG_HOME.
startAllNodes	Starts all the Nodes in a given CONFIG_HOME irrespective of the Node startup mode, that is, Nodes with Manual startup mode are also started in addition to Nodes with Automatic startup mode.   Refer to the "Nodes Reference" table in the "Managing Nodes" section of the <i>TIBCO ActiveMatrix Service Grid Administration Guide</i> .
stopAllHosts	Stops all TIBCO Host Instances in a given CONFIG_HOME.
stopAllNodes	Stops all the Nodes in a given CONFIG_HOME irrespective of the Node startup mode, that is, Nodes with Manual startup mode are also stopped in addition to Nodes with Automatic startup mode.
updateManifest	Updates and fixes the Manifest files of the bundles for accommodating javax.servlet version 3.1.0.
describeHostUpgradeHistory	Provides information about the upgrade history of the specified TIBCO Host instance.
updateWindowsServices	Updates the Host TRA properties in the Windows registry for Host instances running as a Windows service.

### startAllHosts

The "startAllHosts" command starts all TIBCOHost Instances in the specified CONFIG\_HOME. If a TIBCOHost Instance is installed as Windows service, this command starts the instance as a Service.

This command identifies all TIBCO Host instances in the specified CONFIG\_HOME and starts them. Specific TIBCO Host instances can be started by providing the "-instanceNames" argument. "ClearCache" startup can be handled by specifying "-clearCache". This will start Host instances as Services if they are running as Windows NT Service.



This command does not handle "clearCache" start of Hosts running as Windows Service.



By default, this command starts all Hosts instances as soon as possible, that is, it does not wait for a Host to start fully before starting the next Host.



When using the "startAllHosts" command in a setup containing a large number of Nodes (in Automatic startup mode), the "delayInSeconds" parameter must be used to account for the considerable time delay (in seconds) between the TIBCOHosts' startup.

## Arguments

In addition to the common arguments, you can specify the following arguments:

Argument	Description
-configHomeLocation	The location of the CONFIG_HOME.
-instanceName	(Optional) Name of TIBCO Host instance. If this argument is not provided, it starts all TIBCO Host instances in the CONFIG_HOME.
-instanceNames	List of TIBCO Host instance names separated by comma.
-clearCache	Perform "clearCache" startup. It does not handle "clearCache" startup for TIBCOHosts running as Windows Service.
-delayInSeconds	Delay between each TIBCO Host instance startup. This argument is optional. The command uses a default delay of 10 seconds.
-ignoreNodeStartupMode	(Optional) Start all Nodes on the Host irrespective of their startup Mode (Automatic, Manual). If this argument is not provided, it will start all the Nodes with Automatic startup Mode.
-handleOneAtATime	(Optional) Wait for one instance to fully start before starting the next instance. If this argument is not provided, it will start all TIBCO Host instances without wait.
-hostNodeStartMaxWaitTimeInSeconds	(Optional) Defines the maximum Host and Node startup wait time in seconds. If this argument is not provided, a default value of 60 seconds is used.

## Examples

```
>startAllHosts -configHomeLocation /path/to/confighome/location
```

This starts *all* TIBCOHost Instances in the CONFIG\_HOME /path/to/confighome/location.

```
>startAllHosts -configHomeLocation /path/to/confighome/location -clearCache
```

This starts *all* TIBCOHost Instances with "clearCache" in the CONFIG\_HOME /path/to/confighome/location.

```
>startAllHosts -configHomeLocation /path/to/confighome/location -instanceName myTibcoHostInstance
```

This starts the TIBCOHost Instance myTibcoHostInstance in the CONFIG\_HOME /path/to/confighome/location.

```
>startAllHosts -configHomeLocation /path/to/confighome/location -clearCache -delayInSeconds 30
```

This starts *all* TIBCOHost Instances with "clearCache" in the CONFIG\_HOME /path/to/confighome/location and adds delay of 30 seconds between each TIBCOHost startup.

## startAllNodes

The "startAllNodes" command starts all the Nodes in a given CONFIG\_HOME irrespective of the Node startup mode, that is, Nodes with Manual startup mode are also started in addition to Nodes with Automatic startup mode.



A TIBCO Host instance must be running to start the Nodes. The command will verify whether the Host instance is running or not before starting the Nodes.



When using the "startAllNodes" command in a setup containing a large number of Nodes (in Automatic startup mode), the "delayInSeconds" parameter must be used to account for the considerable time delay (in seconds) between the Nodes' startup.

### Arguments

In addition to the common arguments, you can specify the following arguments:

Argument	Description
-configHomeLocation	The location of the CONFIG_HOME.
-instanceName	Name of a TIBCO Host instance. All the Nodes on the specified TIBCO Host instance are started.
-delayInSeconds	(Optional) Delay between each TIBCO Host instance's Node startup. The command uses the default delay of 10 seconds.

### Examples

```
>startAllNodes -configHomeLocation /path/to/confighome/location
```

This starts all Nodes in the CONFIG\_HOME /path/to/confighome/location.

```
>startAllNodes -configHomeLocation /path/to/confighome/location -instanceName myTibcoHostInstance
```

This starts all the Nodes managed by the TIBCOHost Instance "myTibcoHostInstance" in the CONFIG\_HOME /path/to/confighome/location.

```
> startAllNodes -configHomeLocation /path/to/confighome/location -delayInSeconds 30
```

This starts all Nodes in the CONFIG\_HOME /path/to/confighome/location and adds delay of 30 seconds between each Node's startup.

## stopAllHosts

The "stopAllHosts" command stops all TIBCOHost Instances in a given CONFIG\_HOME. Specific TIBCO Host instances can be stopped by providing "-instanceNames" argument.

## Arguments

In addition to the common arguments, you can specify the following arguments:

Argument	Description
-configHomeLocation	The location of the CONFIG_HOME.
-instanceName	Name of TIBCO Host instance.
-instanceNames	(Optional) List of TIBCO Host instance names separated by comma.  If this argument is not provided, it will stop all TIBCO Host instance in the CONFIG_HOME.
-forceStopAllNodes	(Optional) Forcefully stops all Nodes, irrespective of the startup mode or skip Node TRA property.  If this argument is not provided, the startup mode or the skip Node TRA property is considered for stopping Hosts.

## Examples

```
>stopAllHosts -configHomeLocation /path/to/confighome/location
```

This stops *all* TIBCOHost Instances in the CONFIG\_HOME /path/to/confighome/location.

```
>stopAllHosts -configHomeLocation /path/to/confighome/location -instanceName myTibcoHostInstance
```

This stops the TIBCOHost Instance myTibcoHostInstance in the CONFIG\_HOME /path/to/confighome/location.

## stopAllNodes

The "stopAllNodes" command stops all the Nodes in a given CONFIG\_HOME irrespective of the Node startup mode, that is, Nodes with Manual startup mode are also stopped in addition to Nodes with Automatic startup mode.

Nodes on a specific TIBCO Host instance can be stopped by providing the "-instanceName" argument. The TIBCO Host instance must be running to stop the Nodes. The command verifies whether the Host instance is running or not before stopping the Nodes.

## Arguments

In addition to the common arguments, you can specify the following arguments:

Argument	Description
-configHomeLocation	The location of the CONFIG_HOME.
-instanceName	(Optional) Name of TIBCO Host instance. If this argument is not provided, it stops all Nodes on the specified Host in the CONFIG_HOME.

## Examples

```
>stopAllNodes -configHomeLocation /path/to/confighome/location
```

This stops all Nodes in the CONFIG\_HOME /path/to/confighome/location.

```
>stopAllNodes -configHomeLocation /path/to/confighome/location -instanceName myTibcoHostInstance
```

This stops the Nodes managed by TIBCOHost Instance "myTibcoHostInstance" in the CONFIG\_HOME /path/to/confighome/location.

## updateManifest

The "updateManifest" command updates and fixes the Manifest files of the bundles for accommodating the latest javax.servlet version. This command is used while upgrading existing WebApps on the Nodes and for existing installed features on the Host.



The TIBCO Host instances must not be in Running state. That is, all Nodes on the instances must be stopped first to update the manifest.

### Arguments

Argument	Description
-configHomeLocation	The location of the CONFIG_HOME in which the bundles need to be updated.
-instanceNames	List of TIBCO Host instance names separated by a comma. For example "Host1, Host2".
-nodeName	(Optional) The name of the Node for which WebApp is to be updated for the given Host instance.  The command will write to a default log file as needed. If this argument is not provided, all the Nodes managed by that Host will be updated.
-hostPlugins	Updates the javax.servlet dependency of all the features installed on the Host. If provided the command will update the bundles in the Host. This argument cannot be used in conjunction with the -nodeName argument.
-clearCache	(Optional) Clear the cache without starting TIBCO Host instance(s).
-dryRun	Allows you to see what changes would be made by this command by inspecting the log, without making the actual changes.

### Examples

The following command updates the Manifest files of the bundles for accommodating the latest javax.servlet version. This command is used while upgrading existing WebApps on the Nodes.

```
updateManifest -configHomeLocation path/to/CONFIG_HOME/location -instanceName myTibcoHostInstance
```

If -hostPlugins is used, it updates and fixes the Manifest files of the bundles for accommodating the latest javax.servlet version. This command is used for existing installed features on the Host.

```
updateManifest -configHomeLocation path/to/CONFIG_HOME/location -instanceName myTibcoHostInstance -hostPlugins
```

## describeHostUpgradeHistory

The "describeHostUpgradeHistory" command provides information about the upgrade history of the specified TIBCO Host instance.

The following command describes the upgrade history for a ActiveMatrix Administrator directory.

```
> describeHostUpgradeHistory -adminServerDir path/to/server/directory
```

The following command describes the upgrade history for a particular instance of the CONFIG\_HOME.

```
> describeHostUpgradeHistory -configHomeLocation path/to/CONFIG_HOME/location -instanceName myTibcoHostInstance
```

## Arguments

See [Common Arguments](#).

### Example: upgrade history of ActiveMatrix Administrator directory

Command:

```
E:\tibco\amx\3.4\bin>tibamx_hostmanager.exe describeHostUpgradeHistory -adminServerDir E:\tibco\config1\admin\amxadmin\private\instanceOne
```

A sample output is shown below:

```
Invoking describeHostUpgradeHistory
-adminServerDir E:\tibco\config1\admin\amxadmin\private\instanceOne

Upgrade history, current to oldest:
  Host platform version: 3.2.0, no associated patch(es)
  Host platform version: 3.4.0, associated patch(es): amx.platform.patch:3.4.0
  Host platform version: 3.2.0, no associated patch(es)
Host can be Downgraded:
```

### Example: upgrade history of an instance of CONFIG\_HOME

Command:

```
E:\tibco\amx\3.4\bin>tibamx_hostmanager.exe describeHostUpgradeHistory -configHomeLocation E:\tibco\config1 -instanceName Admin-amxadmin-instanceOne
```

A sample output is shown below:

```
Invoking describeHostUpgradeHistory
-configHomeLocation E:\tibco\config1
-instanceName Admin-amxadmin-instanceOne

Upgrade history, current to oldest:
  Host platform version: 3.4.0, associated patch(es): amx.platform.patch:3.4.0
  Host platform version: 3.3.0.HF15, associated patch(es):
amx.platform.patch:3.3.0.HF15
  Host platform version: 3.3.0, no associated patch(es)
Host can be Downgraded:
  3.3.0.HF15
```

## updateWindowsServices

The "updateWindowsServices" command identifies all TIBCO Host instances in the specified CONFIG\_HOME and updates the Host TRA properties in the Windows registry for TIBCO Host instances running as a Windows service.



This command updates the TRA properties only for TIBCO Host instances running as a Windows Service. It updates TRA properties for a specific Host instance if the instance name is provided.

## Arguments

See [Common Arguments](#). In addition to the common arguments, you can specify the following arguments:

Argument	Description
-configHomeLocation	The location of CONFIG_HOME.
-instanceName	(Optional) Name of TIBCO Host instance running as a Windows service, for which the TRA properties in the Windows registry need to be updated.

### Examples

- The following command identifies all TIBCO Host instances in the specified CONFIG\_HOME and updates their TRA properties in the Windows registry.  

```
updateWindowsServices -configHomeLocation path/to/CONFIG_HOME/location
```
- The following command updates the TRA properties of the specified instance name in the Windows registry.  

```
updateWindowsServices -configHomeLocation path/to/CONFIG_HOME/location -instanceName my-instance
```

## Miscellaneous Commands

The following miscellaneous commands are available:

Command	Description
clearLog	Deletes the log file. The default log file is located in CONFIG_HOME\tibamx_hostmanager\logs\tibamx_hostmanager.log.
interactive	Enters an interactive shell. The Interactive command loop is useful for invoking multiple commands without re-running the tool.
intro	Displays a detailed description of the Host Manager, its purpose, and use.
version	Displays the version of Host Manager.
viewLog	Displays the contents of a log file on the console.

## Common Arguments

The following arguments are applicable to all commands listed in the previous sections.

Argument	Description
-configFile	(Optional) The location of a configuration file that can pre-configure the arguments.  The default configuration file is TIBCO_HOME\amx\3.3\scripts\tibamx_hostmanager.properties.

Argument	Description
-installLocation	(Optional) The location of a TIBCO_HOME folder from which patches are copied.  Default: TIBCO_HOME in which the Host Manager was installed.
-logFile	(Optional) The location of a log file to which command execution can be logged. If this argument is not provided, the command writes to a default log file as needed.  The default log file is CONFIG_HOME \tibamx_hostmanager\logs \tibamx_hostmanager.log.
-stackTrace	(Optional) When this argument is specified, a stack trace is shown upon encountering exceptions during command execution. If this argument is not provided, the stack traces are suppressed.
-showTimeStamp	(Optional) When this argument is specified, the execution output shows timestamps. If this argument is not provided, the timestamp is not shown.

### Examples

- Example of "-logFile":

```
>startAllHosts -configHomeLocation /path/to/confighome/location -clearCache -logFile /path/to/logfile
```

- Example of "-showTimeStamp":

```
>startAllNodes -configHomeLocation /path/to/confighome/location -showTimeStamp
```

- Example of "-stackTrace":

```
>stopAllHosts -configHomeLocation /path/to/confighome/location -stackTrace
```

Some of the other common arguments used by Host Manager Commands include:

Argument	Description
-adminServerDir	The location of an Administration Server Host configuration folder. The folder is located under a CONFIG_HOME folder, in admin/<enterprise>/private/<system host instance name>.
-configHomeLocation	The location of a CONFIG_HOME where the TIBCO Host instance to be described exists.
-instanceName	The name of the TIBCO Host instance to be described.
-ID	A patch identifier which all shell commands will use by default. Identifiers are of the form <name>:<version>.

Argument	Description
-dryRun	Allows you to see what changes would be made by this command, without making the actual changes. The command executes without making changes and you can look in the log to see what changes would have been made.  The default value is false.

## clearLog

The "clearLog" command deletes the log file. If no log file is specified, the default log file is deleted. The default log file is located in CONFIG\_HOME\tibamx\_hostmanager\logs\tibamx\_hostmanager.log.

### Arguments

See [Common Arguments](#). In addition to arguments that are common across all commands, the following arguments can be specified:

Argument	Description
-configHomeLocation <path>	The location of a CONFIG_HOME folder where the log file to be deleted exists.

### Example

```
clearLog -configHomeLocation path/to/CONFIG_HOME/location
```

## interactive

The "interactive" command enters an interactive shell.

The Interactive command loop is useful for invoking multiple commands without re-running the tool. If you invoke Host Manager commands within the loop, all the commands share the configuration provided initially to the command loop. You can also change the loop configuration while running in the loop.

The following commands are available from the shell:

Command	Description
getConfiguration	View the configuration properties used in the shell.
changeConfiguration	Change the configuration properties used in the shell.
exit	Exit the shell.

### Arguments

See [Arguments identifying hosts being upgraded](#).

### Examples

- `interactive -adminServerDir path/to/CONFIG_HOME/location -ID my.patch:1.2.3`



- `interactive -configHomeLocation path/to/CONFIG_HOME/location -instanceName my-instance`

## intro

The "intro" command displays a detailed description of the Host Manager, its purpose, and use.

### Arguments

None

### Example

```
> intro
```

## version

The "version" command displays the version of Host Manager.

### Arguments

None

### Example

```
> version
```

The command displays the version of the Host Manager. For example:

```
TIBCO ActiveMatrix Host Manager version 2.0.5
```

## viewLog

The "viewLog" command displays the contents of a log file on the console. If no log file is specified, the default log file contents are displayed. The location of the log file and a time-stamped list of all operations that have been performed is listed.

### Arguments

See [Common Arguments](#). In addition to arguments that are common across all commands, the following arguments can be specified:

Argument	Description
<code>-configHomeLocation &lt;path&gt;</code>	The location of a CONFIG_HOME folder where the log file to be viewed exists. Must be specified if the <code>-logfile</code> argument is not.

### Example

```
>viewLog -configHomeLocation path/to/CONFIG_HOME/location
```

## installInfo

The "installInfo" command displays information about products, hotfixes, and engineering builds from the current TIBCO\_HOME or a specific TIBCO\_HOME. For products and hotfixes, the information is retrieved from the `_installInfo` folder. For engineering builds, the information is retrieved from the `_ebInstallInfo` folder.

The command also creates an XML file named `installinfo.xml` in the specified or current TIBCO\_HOME with all the details.

## Arguments

See [Common Arguments](#). In addition to arguments that are common across all commands, the following arguments can be specified:

Argument	Description
-tibcoHome <path>	The location of the TIBCO_HOME folder for which the information needs to be retrieved.

### Example 1

```
> installInfo
```

The command displays details of the current TIBCO\_HOME. For example:

```
ProductDescription: TIBCO ActiveMatrix Service Grid 3.4.0
ProductVersion: 3.4.0.000
ProductID: amsg
```

The following XML file is created in the current TIBCO\_HOME:

```
<products>
  <product ProductDescription="TIBCO ActiveMatrix Service Grid 3.4.0" ProductID="ams">
    <ProductVersion>3.4.0.000</ProductVersion>
  </product>
</products>
```

### Example 2

```
installInfo -tibcoHome <TIBCO_HOME>
```

The command displays details of installations in the specified TIBCO\_HOME (from the \_installInfo folder) and engineering builds installed in the specified TIBCO\_HOME (from the \_ebInstallInfo folder).

```
ProductDescription: TIBCO ActiveMatrix Service Grid 3.3.0
ProductVersion: 3.3.0.000
ProductID: amsg
ProductDescription: TIBCO ActiveMatrix Service Grid 3.4.0
ProductVersion: 3.4.0.000
ProductID: amsg
ProductDescription: TIBCO ActiveMatrix® BPM 4.0.0 Hotfix 1
ProductVersion: 4.0.0.001
ProductID: amx-bpm
ProductDescription: TIBCO ActiveMatrix® BPM 4.0.0
ProductVersion: 4.0.0
ProductID: amx-bpm
ProductDescription: TIBCO Hawk® 5.2.0
ProductVersion: 5.2.0
ProductID: hawk
ProductDescription: TIBCO ActiveMatrix Platform 3.3.0 Hotfix-017
ProductVersion: 3.3.0.017
ProductID: hf-amx330-prod
ProductDescription: TIBCO ActiveMatrix Engineering Build
ProductVersion: AMX_3.3.0_ENGINEERING_BUILD10
ProductID: EB
```

The following XML file is created in the specified TIBCO\_HOME:

```

▼<products>
  ▼<product ProductDescription="TIBCO ActiveMatrix Service Grid 3.3.0" ProductID="amsg">
    <ProductVersion>3.3.0.000</ProductVersion>
  </product>
  ▼<product ProductDescription="TIBCO ActiveMatrix Service Grid 3.4.0" ProductID="amsg">
    <ProductVersion>3.4.0.000</ProductVersion>
  </product>
  ▼<product ProductDescription="TIBCO ActiveMatrix ® BPM 4.0.0 Hotfix 1" ProductID="amx-bpm">
    <ProductVersion>4.0.0.001</ProductVersion>
  </product>
  ▼<product ProductDescription="TIBCO ActiveMatrix ® BPM 4.0.0" ProductID="amx-bpm">
    <ProductVersion>4.0.0</ProductVersion>
  </product>
  ▼<product ProductDescription="TIBCO Hawk 5.2.0" ProductID="hawk">
    <ProductVersion>5.2.0</ProductVersion>
  </product>
  ▼<product ProductDescription="TIBCO ActiveMatrix Platform 3.3.0 Hotfix-017" ProductID="hf-amx330-prod">
    <ProductVersion>3.3.0.017</ProductVersion>
  </product>
  ▼<product ProductDescription="TIBCO ActiveMatrix Engineering Build" ProductID="EB">
    <ProductVersion>AMX_3.3.0_ENGINEERING_BUILD10</ProductVersion>
  </product>
</products>

```

## Updating JRE Version

The TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) is a command-line utility for updating existing TIBCO ActiveMatrix platform based installations to use JRE 1.8. The utility operates against the CLASSPATH .tra files in TIBCO\_HOME. In the given TIBCO\_HOME, the utility operates only on the CLASSPATH .tra files that are relevant and known to the TIBCO ActiveMatrix Platform based products.



When you obtain third party software or services, it is your responsibility to ensure you understand the license terms associated with such third-party software or services and comply with such terms.

### Modes

The utility works in two modes:

- Discover mode — Discovers the various "TIBCO ActiveMatrix Administrator Instances" for a given TIBCO\_CONFIG\_HOME.
- Update mode — For a given TIBCO\_HOME, this mode updates the Java version in the relevant TIBCO ActiveMatrix .tra files in TIBCO\_HOME.

## Approach

In all TIBCO ActiveMatrix installations, the path to JRE home is specified in the CLASSPATH .tra files in the TIBCO\_HOME directory. When a new TIBCO Host is created, a TIBCO\_CONFIG\_HOME directory is created, and all the host and node files in this TIBCO\_CONFIG\_HOME directory point to the CLASSPATH .tra files in the corresponding TIBCO\_HOME directory.

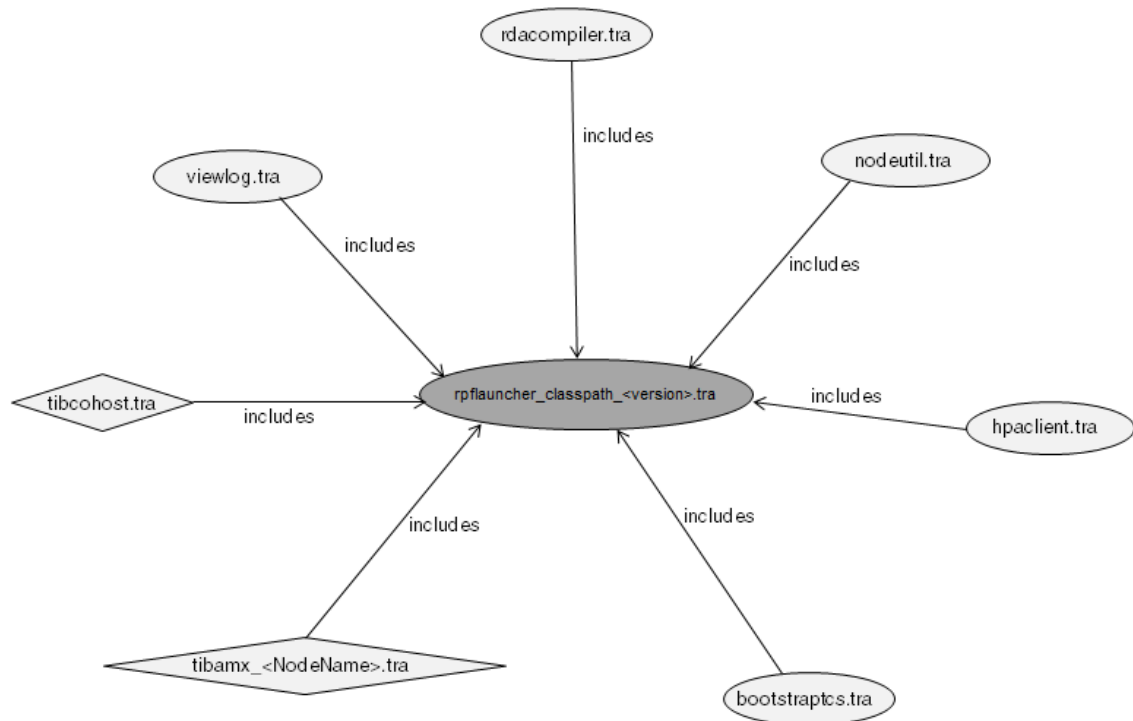


- One or more TIBCO\_CONFIG\_HOME directories can point to the same TIBCO\_HOME directory.
- A single TIBCO\_CONFIG\_HOME can contain multiple "TIBCO ActiveMatrix Administrator Instances" pointing to different TIBCO\_HOME directories.

The following diagram illustrates the relationship between the files in the two directories. In this diagram, the:

- Diamond shaped nodes are from TIBCO\_CONFIG\_HOME and oval shaped are from TIBCO\_HOME.
- Dark colored nodes are modified during the update to JRE 1.8.

## Current release of ActiveMatrix



Updating the JRE path in the common CLASSPATH .tra files in the TIBCO\_HOME directory updates the JRE version for all the hosts and nodes in the TIBCO\_CONFIG\_HOME directories pointing to it. Any new node instance created after that will also use JRE 1.8.



The TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) updates files at TIBCO\_HOME level, and not at an individual TIBCO\_CONFIG\_HOME level. This means that when .tra files in TIBCO\_HOME are updated all the tibcohosts and nodes in different TIBCO\_CONFIG\_HOMEs that point to a particular TIBCO\_HOME will be automatically updated to use JRE 1.8.

## Properties Updated in CLASSPATH .tra Files

The following is a list of JRE properties in the CLASSPATH .tra files which are updated by the TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) for a simple installation of the TIBCO ActiveMatrix platform:

```
TIBCO_HOME/amx/<version>/scripts/rpflauncher_classpath_<version>.tra :
[java.library], [tibco.env.PATH], [tibco.env.LIBPATH]
```

### Multiple Product Installation

If multiple products are installed in the same TIBCO\_HOME, this utility can be run multiple times with different include files each time, specific to the different products. Multiple runs of this tool do not affect the .tra and .ini files, which have already been modified.

## Invoking the Tool

### Prerequisites

- Before running TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE), shutdown the tibcohost instance you are managing to avoid severe errors by running the "tibcohost stop - wait true" command. The TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) does NOT verify that the tibcohost is shut down.

- When run in the update mode, the JRE Updater tool only updates files in the TIBCO\_HOME from which it is run. However, in the discover mode, it discovers all tibcohost and node instances in a TIBCO\_CONFIG\_HOME irrespective of which TIBCO\_HOME they point to.
- The operation of the utility depends on the location from where the utility is being run. For example, if the tool is run from \$TIBCO\_HOME/amx/3.4/bin/, only the tibcohost and node instances that are of version 3.4.0 are discovered.
- The bit version of the JRE to which you are upgrading must match the bit version of the operating system architecture.

## Modes

- Interactive Mode (default) — To execute the TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) in the interactive mode, run the following command from <TIBCO\_HOME>/amx/<version>/bin/.

- amx\_jre\_updater.exe (Microsoft Windows)
- ./amx\_jre\_updater (UNIX)

The tool enters an interactive shell where you can execute all TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) commands, including any command specific arguments. The exit command exits the shell.

- Non-interactive Mode — To execute the TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) in a non-interactive (scripted) mode, run the following from <TIBCO\_HOME>/amx/<version>/bin/:

- ./amx\_jre\_updater <command> -jreHome <JRE\_HOME\_PATH> <Optional arguments> (UNIX)
- amx\_jre\_updater.exe <command> -jreHome <JRE\_HOME\_PATH> <Optional arguments> (Microsoft Windows)

where <command> is one of the TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) commands, followed by command specific arguments.



- For the -jreHome argument, provide the JRE\_HOME (and not the JDK\_HOME) bundled inside the JDK. If you point to JDK\_HOME, the path updated for tra/ini does not work for Runtime.
- The tool uses the existing JRE when it is invoked. The tool's own TRA is updated during every update operation.

## Help Commands

All commands in the TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) are documented within the tool:

- Use the help command to get a list of all available commands

- amx\_jre\_updater.exe help (Microsoft Windows)
- ./amx\_jre\_updater help (UNIX)

In the interactive mode, use: help

- Use help <command> to get detailed help on a specific command, including command examples:


- amx\_jre\_updater.exe help <command> (Microsoft Windows)
- ./amx\_jre\_updater help <command> (UNIX)

In the interactive mode, use: help <command>

- Use `help jreUpdaterCommands` to get detailed help on common command arguments:
    - `amx_jre_updater.exe jreUpdaterCommands` (Microsoft Windows)
    - `./amx_jre_updater jreUpdaterCommands` (UNIX)
- In the interactive mode, use: `jreUpdaterCommands`

## Modes of Operation

The TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) works in two modes:

- Discover mode — Discovers the various "TIBCO ActiveMatrix Administrator Instances" for a given `TIBCO_CONFIG_HOME`.
  - Update mode — For a given `TIBCO_HOME`, this mode updates the Java version in the relevant TIBCO ActiveMatrix .tra files in `TIBCO_HOME`. The affected .tra files are not just those that are included by hosts and nodes, but also those tools known to TIBCO ActiveMatrix Platform based products. The output is a list of the affected .tra files, hosts, and nodes.
- 
  - The update affects all instances of `TIBCO_CONFIG_HOME` that are pointing to that particular `TIBCO_HOME`.
  - After updating the `TIBCO_HOME` to use JRE 1.8, if any new `tibcohost` or `node` instances are created, they will use JRE 1.8 by default.

## Commands

Command	Description
<code>help</code>	Provides a list of all available commands.
<code>help &lt;command&gt;</code>	Provides detailed information on a particular command.
<code>discover</code>	Discover the various "TIBCO ActiveMatrix Administrator Instances" for a given <code>TIBCO_CONFIG_HOME</code> .
<code>update</code>	Updates the specified <code>TIBCO_HOME</code> to the specified <code>JRE_HOME</code> path.
<code>intro</code>	Displays a detailed description including the purpose and use of the TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE).
<code>version</code>	Displays the version of the TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE).

Command	Description
viewLog	<p>The tool maintains a detailed log of all changes associated with a particular update operation.</p> <p>The viewLog command display the contents of a log file to the console.</p> <p>If no log file is specified, the default log file contents are displayed.</p> <p>The default log file is TIBCO_HOME/tibamx_jreupdater/logs/tibamx_jreupdater.log.</p> <pre>viewLog -logFile &lt;path&gt;</pre> <p>where &lt;path&gt; is the location of the log file to be viewed.</p> <p>Example:</p> <pre>viewLog -logFile C:\test\logFile.log</pre>
clearLog	<p>Clears the log file. If no log file is specified, the default log file is cleared.</p> <pre>clearLog -logFile &lt;path&gt;</pre> <p>where &lt;path&gt; is the location of the log file to be cleared.</p> <p>Example:</p> <pre>clearLog -logFile C:\test\logFile.log</pre>

## Discover Mode

The discover command discovers the various "TIBCO ActiveMatrix Administrator Instances" for the specified TIBCO\_CONFIG\_HOME. The syntax of the command is:

```
discover -configHomeLocation <path>
```

Where <path> is the location of the TIBCO\_CONFIG\_HOME folder where the TIBCO Host instance to be updated exists.

Example:

```
discover -configHomeLocation /path/to/confighome/location
```

In the output, the ActiveMatrix Administrator instances are grouped based on the TIBCO\_HOME version.

### Example

```
> discover -configHomeLocation "E:\tibco\config1"
```

The output is:

```
Following is a list of Admin Enterprise Instances
  TIBCO_HOME Location: E:\tibco
    JRE_HOME Location: C:\Program Files\Java\jre1.8.0_181
    AMX Version: 3.4.0
    Admin-amxadmin-instanceOne
      Node Names:
        DevNode
        SystemNode
```



## Update Mode

The Update command updates the JRE for a given TIBCO\_HOME and all the "TIBCO ActiveMatrix Administrator Instances" referencing it. Specify the JRE\_HOME location. JRE is updated for the TIBCO\_HOME, from which the tool is invoked.



For TIBCO ActiveMatrix 3.2.0, the JRE updater tool needs to be installed separately. For TIBCO ActiveMatrix 3.4.0, the tool is installed by default in <TIBCO\_HOME>\amx\3.4\bin\amx\_jre\_updater\.. When you upgrade from 3.2.0 to 3.4.0, you must run the utility from the directory of the higher version (for example, <TIBCO\_HOME>/amx/3.4/) and not the lower version (for example, <TIBCO\_HOME>/amx/3.2/).

The general syntax of the command is:


```
update -jreHome <path to JRE> -updateIni -dryRun
```

The -dryRun option only lists the files that will be updated. It does not modify any files. To modify the files, run the update command without the -dryRun option.

Example:

```
update -jreHome C:/test/amx3/PlatformSupport/<JDK version>/jre -updateIni
```

### Arguments of Update Command

Argument	Description
-jreHome <path>	<p>The path to the JRE_HOME to which you want to update.</p> <div>  <p>Provide the JRE_HOME (and not the JDK_HOME) bundled inside the JDK. If you point to JDK_HOME, the path updated for tra/ini does not work for Runtime.</p> </div>
-includeFile <include-file-path>	<p>The path to the file containing the list of .tra or .ini files to be included in the update process.</p> <p>The path in the file can be an absolute path or relative to TIBCO_HOME.</p> <p>Sample content in the include file:</p> <pre>TIBCO_HOME/a TIBCO_HOME/b TIBCO_HOME/c/d /home/AMX-products/AMX3x-HFs/e/f</pre> <p>Where a, b, c and d are the name of folders which gets created for products other than TIBCO ActiveMatrix.</p>

Argument	Description
<code>-excludeFile &lt;exclude-file-path&gt;</code>	<p>The path to the file containing the list of .tra or .ini files to be excluded in the update process.</p> <p>The path in the file can be an absolute path or relative to TIBCO_HOME.</p> <p>Sample content in the exclude file:</p> <pre>TIBCO_HOME/a TIBCO_HOME/b TIBCO_HOME/c/d /home/AMX-products/AMX3x-HFs/e/f</pre> <p>Where a, b, c and d are the name of folders which gets created for products other than TIBCO ActiveMatrix.</p>
<code>-updateIni</code>	<p>This argument is applicable only with version 3.2.0, 3.3.0, and 3.3.1. The default value is false. If set, the command also updates the .ini files in the specified TIBCO_HOME.</p>
<code>-dryRun</code>	<p>Optional argument; default value is false. If set, the command does not make any changes. It only displays information on what would have been done.</p>
<code>-configFile &lt;path&gt;</code>	<p>The location of a configuration file that can preconfigure the command.</p> <p>This argument is optional.</p> <p>Sample content in the configuration file:</p> <pre>tibamx_jreupdater.DefaultJreHome=/a/b/c/jdk1.8.0_31/ jre tibamx_jreupdater.DefaultConfigHomeLocation=/a/b/c/d tibamx_jreupdater.DefaultIncludeFile=a/b/c/ includeFile.txt tibamx_jreupdater.DefaultExcludeFile=a/b/c/ excludeFile.txt</pre>
<code>-logFile &lt;path&gt;</code>	<p>The location of a log file that keeps track of command execution. This argument is optional; commands write to a default log file as needed.</p>
<code>-stackTrace</code>	<p>Creates a full exception stack trace on encountering an error. This argument is optional.</p>

### Example

```
E:\tibco\AMXTestInstaller\amx\3.4\bin>amx_jre_updater.exe update -jreHome
"C:\Program Files\Java\jre1.8.0_181" -updateIni -dryRun
```

The output of the command is as follows:

```
File 'E:\tibco\amx\3.4\scripts\rpflauncher_classpath_3.4.0.tra' has been modified:
JRE.HOME in property [java.library] has been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\amx\3.4\scripts\rpflauncher_classpath_3.4.0.tra' has been modified:
JRE.HOME in property [tibco.env .PATH] has been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\amx\3.4\bin\TIBCOConfigurationTool.ini' has been modified: [E:/tibco/
```

```

tibcojre64/1.8.0] has be
en changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\amx\3.4\bin\TIBCOConfigurationToolc.ini' has been modified: [E:/
tibco/tibcojre64/1.8.0] has b
een changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\studio\5.0\eclipse\amx_eclipse_ant.tra' has been modified: JRE.HOME
in property [java.library] has
been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\studio\5.0\eclipse\amx_eclipse_ant.tra' has been modified: JRE.HOME
in property [tibco.env.PATH] ha
s been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\studio\5.0\eclipse\TIBCOBusinessStudio.ini' has been modified: [E:/
tibco/tibcojre64/1.8.0] ha
s been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\tct\1.6\TIBCOConfigurationToolc.ini' has been modified: [E:/tibco/
tibcojre64/1.8.0] has been c
hanged to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\tct\1.6\TIBCOConfigurationToolc.ini' has been modified: [E:/tibco/
tibcojre64/1.8.0] has been
changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\amx_it_mediation\3.5\bin\AutoMediate.tra' has been modified:
JRE.HOME in property [tibco.env.TIBCO_
JVM_LIB_DIR] has been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\amx_it_mediation\3.5\bin\AutoMediate.tra' has been modified:
JRE.HOME in property [tibco.env.PATH]
has been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\amx_it_mediation\3.5\bin\AutoMediate.tra' has been modified:
JRE.HOME in property [java.library] ha
s been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\amx_it_mediation\3.5\samples\Util\bin\samplesdb.tra' has been
modified: JRE.HOME in property [tibco
.env.TIBCO_JVM_LIB_DIR] has been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\amx_it_mediation\3.5\samples\Util\bin\samplesdb.tra' has been
modified: JRE.HOME in property [tibco
.env.PATH] has been changed to C:\Program Files\Java\jre1.8.0_181
File 'E:\tibco\amx_it_mediation\3.5\samples\Util\bin\samplesdb.tra' has been
modified: JRE.HOME in property [java.
library] has been changed to C:\Program Files\Java\jre1.8.0_181

```

## Reverting to the Previous Version of the JRE



For 3.3.1, you cannot revert to an older version of Java.

- To revert to a previous version of the JRE, invoke the tool with the intended JRE\_HOME as argument.

```
update -jreHome <path>
```



You cannot use this command to revert to an externally installed version of JRE 1.6. For that, you must use the "update -jreHome TIBCO\_JRE" command.

- To revert to tibcojre, specify TIBCO\_JRE as the value for the argument -jreHome.

```
update -jreHome TIBCO_JRE
```

## Backup of Files

The TIBCO ActiveMatrix Updater Tool for Java Runtime Environment (JRE) backs up all the .tra and .ini files that are updated during the JRE update process.

The .bak files are stored in the same location as the original .tra or .ini file. The existing .tra or .ini file is renamed as: <Existing\_Name>\_<Time-Stamp>.bak.



- The time stamp value is the same for all the .bak files in a given update process.
- In one update operation, the time stamp for each and every .tra and .ini file is the same.

## Logging

The default log file is located at `TIBCO_HOME/tibamx_jreupdater/logs/tibamx_jreupdater.log`.

To specify a different log file location, execute the following command:

```
update -logFile <new path>
```

# Troubleshooting

If you encounter problems with installation, make sure that your system meets all prerequisites. Next, check the installer log file for potential problems.

## Non-Administrator Users Encounter TCT File Lock Error Message

### Problem

Non-administrator users see the following message while running the TIBCO Configuration Tool (TCT) to configure TIBCO ActiveMatrix Administrator Server: "TIBCO-AMX-INFRA00193: Machine file at file:/TIBCO\_HOME/tools/machinemodel/shared/version/machine.xmi could not acquire the lock; it is locked by *file name*".

### Workaround

Provide administrator privileges to user.

## CONFIGURE\_FAILED Message in Single Machine Setup

### Problem

During development, you install all components on a single machine. After the Administrator server configuration, select TIBCO Adapter Implementation Type App Template from the list of application templates to deploy on the default node. A CONFIGURE\_FAILED message results.

### Workaround

Installation instructions clearly state not to select this option. Because the TIBCO Hawk Agent workflow is not run at this time, deployment of this component results in a startup failure with a CONFIGURE\_FAILED message.

## Installing ActiveMatrix Using a Non-default Administrator Account

### Scenario

This is a scenario on Windows 2008 or Windows 7 when the product is installed using a non-default Administrator user. Assume you have two accounts: Administrator, which was created at the operation system setup, and tibco, which was created afterwards and added to Administrator group. As a result, tibco is considered as a non-default Administrator. With a non-default Administrator, there are some issues you might encounter:

Problem	Resolution
The file, machine.xmi, is locked when you create TIBCO ActiveMatrix Administrator Server using TIBCO Configuration Tool.	Start TIBCO ConfigurationTool.exe with the <b>Run As Administrator</b> option.
Access is denied while starting or stopping TIBCO Host from the command-prompt.	Start the command prompt using the <b>Run as Administrator</b> option.

## Edit ActiveMatrix Administrator Server Configuration using TCT to make ActiveMatrix Administrator SSL enabled. Configuring ActiveMatrix Policy Director Governance on this setup fails.

### Problem

ActiveMatrix Administrator with SSL disabled is installed in <CONFIG\_HOME>. ActiveMatrix Administrator Server Configuration is edited using TCT to make ActiveMatrix Administrator SSL

enabled. Configuring ActiveMatrix Policy Director Governance on this setup fails because of SSL keystore location is not detected.

### Workaround

When editing configuration of ActiveMatrix Administrator Server using TCT, change the location of **Session Scripts and Log Folder** from `<CONFIG_HOME>/tct/admin.editor/<date-time>` to `<CONFIG_HOME>/tct/admin/<date-time>` in **Administration Server Configuration: Summary** screen.

## ActiveMatrix Administrator Not Starting Due to Database Connection Failure

### Problem

The ActiveMatrix Administrator server is not starting, or you are unable to login due to database connection failure.

### Workaround

Perform the following procedure to update database configuration:

1. Start the SystemNode and tibcohost, if stopped, even if the ActiveMatrix Administrator is not working.
2. In your database server, unlock the user account. When several failed attempts are made at entering a password, ActiveMatrix locks an account. This is often encountered while using ActiveMatrix Administrator with Oracle, especially if an expired password has been changed.



For Oracle, you can unlock a user account by executing the following command in sqlplus as a DBA:

```
SQL> alter user <username> account unlock;
```

3. Launch TIBCO Configuration Tool, update the database configuration for the core ActiveMatrix Administrator as follows:
  - a. Select **Edit TIBCO ActiveMatrix Administrator Server Configuration**.
  - b. From the Select Server Configuration drop-down list, select the enterprise name and server name.
  - c. Check **Edit Database Settings**.
  - d. If the users or groups are defined in the Administrator database and not in an LDAP server, select **Edit Authentication Realm Settings**.
  - e. Click **Test Connection** to verify the settings.
  - f. Click **Configure** to apply the changes. When the update is complete, TIBCO Configuration Tool restarts the system node.
  - g. Wait for a few minutes for the system node to become available.
4. Login to ActiveMatrix Administrator UI, and perform the following steps:
  - a. Navigate to **Shared Objects > Resource Templates**, and select **TIBCO ActiveMatrix Governance JDBC Resource**.



Select **GovernanceJDBCSharedResource** if you upgraded from a prior version. If you do not see this resource template, it means monitoring services were not deployed, and hence you can skip this step.

- b. In the details section of this resource template, make corrective changes to the configuration, if needed and save the changes.
- c. Reinstall resource instances and restart applications.

- d. From the **Resource Instances** tab of the details section, verify that the resource instance is successfully installed and is in the *Running* state. There will be multiple resource instances if you have a replicated Administrator.
5. Repeat step 4 for the Resource Templates - **TIBCO ActiveMatrix LogService JDBC Resource** and **TIBCO ActiveMatrix PayloadService JDBC Resource**.



If you upgraded from prior releases, the names will be `cl_logservice_jdbc` and `payloadJdbcSharedResource`. If you do not see these resource templates, it means common logging services were not deployed, and hence you can skip this step.

6. Restart the SystemNode one more time using the following `tibcohost` commands:
  - a. To stop `tibcohost (.exe)`: `stopNodes -nodeName SystemNode`. Wait for a few minutes for a graceful shutdown.
  - b. To start `tibcohost (.exe)`: `startNodes -nodeName SystemNode`. Wait for a few minutes for the SystemNode to come up.

After the restart, the new database settings are fully in effect.

## JRE Updater

**The TIBCO\_HOME is corrupted and I am unable to invoke the JRE Updater tool again.**

Replace `TIBCO_HOME/amx/3.x/bin/amx_jre_updater.tra` with the backup of the `.tra` file created during the last update operation. Invoke the tool and update the `JRE_HOME` again.

**I do not want to upgrade a selected set of `.tra` or `.ini` files. What should I do?**

By default, all the `.tra` files inside `TIBCO_HOME` are updated in any "update" operation irrespective of the TIBCO ActiveMatrix platform version. If you do not want to upgrade any specific `.tra` or `.ini` file, exclude that file using the `-excludeFile` argument.

## Upgrade or Downgrade

**After downgrading from 3.4.0, HTTP Connector resource instances are in the "Installed (Start Failed)" and Applications using them are in "Start Failed" State.**

**Applications**

Name	Application State	Last Deployed On	Synchronization	Action History
System jv.helloworld1.soa	Start failed	2017-07-27 12:36:33	In Sync	Deploy with Start Successful

**HelloConn331**

General | SSL | Advanced | **Resource Instances**

View: HTTP Connector

Instance Name	Type	Template Name	Scope	Instance State	Synchronized	N
hello1Connector	HTTP Connector	HelloConn331	Global	Installed (Start Failed)	In Sync	D

If an HTTP Connector is created in 3.4.0 and you downgrade to a release prior to 3.4.0, the HTTP Connector properties introduced in 3.4.0 will not get applied to the downgraded version of the HTTP Connector Resource Instance. The HTTP Connector Resource Instance will go to the *Installed (Start Failed)* state and the application referring to the HTTP Connector Resource Instance will go to *Start Failed* state. Uninstalling the HTTP connector Resource Instance is not enough in this case. You must recreate the HTTP Connector Resource Template and map the Application to the newly created the HTTP Connector Resource instance corresponding to the HTTP Connector Resource Template.

### The Node Tab in the ActiveMatrix Administrator UI does not show version.

After upgrading or downgrading the Enterprise, clear the browser cache before loading ActiveMatrix Administrator UI. This is required to load some of the new enhancements made in the UI.

### Runtime is upgraded but Administrator is not updated with the changes in runtime.

If a Host or Node is upgraded or downgraded successfully in runtime, but ActiveMatrix Administrator is still showing the version before upgrade or downgrade, the task `syncupWithRuntime` in `Host_build.xml` and `Node_build.xml`, which are available in `TIBCO_HOME/administrator/<version>/samples`, can be used to update Host and Node in Administrator. Samples of build and data file for Host and Node are shown below.

#### Host\_build.xml

```
<targetname="syncupWithRuntime">
  <ActiveMatrixAdminTask
    remote="true"
    propsFile="${instanceProperties}"
    action="syncupWithRuntime"
    dataFile="${dataFile}"
    objectSelector="Host"
    overwrite="true"
    merge="true"
    createIfNotExists="true"
    force="true"
    failOnError="false"
  />
</target>
```

#### Host\_data.xml

```
<Host xsi:type="amxdata:Host" name="SecondHost"
managementUrl="service:jmx:jmxmp://localhost:36923">
<Version old="3.3.1" new="3.4.0"/>
</Host>
```

#### Node\_build.xml

```
<targetname="syncupWithRuntime">
  <ActiveMatrixAdminTask
    remote="true"
    propsFile="${instanceProperties}"
    action="syncupWithRuntime"
    dataFile="${dataFile}"
    objectSelector="Environment/Node"
    force="true"
    failOnError="false"
  />
</target>
```

#### Node\_data.xml

```
<Environment xsi:type="amxdata:Environment" name="DevEnvironment"
contact="TIBCO">
  <Node xsi:type="amxdata:Node" name="DevNode"
HostName="SystemHost" >
    <Version old="3.3.1" new="3.4.0"/>
  </Node>
</Environment>
```



## System Host Downgrade Fails

During downgrade of ActiveMatrix Administrator, ensure that all the Hosts and Nodes in an Enterprise are downgraded or are in the process of downgrading along with the System Host. If any Host is not yet downgraded, the ActiveMatrix Administrator (System Host) downgrade is aborted. If there are other Hosts in the same CONFIG\_HOME, they also go through the downgrade process. In such a scenario, you must fix the cause of the System Host failure first and then try to downgrade again.

**After upgrading to 3.4.0, if the ActiveMatrix Administrator is SSL enabled, it does not load in the latest browser and the connection cipher suite does not display the correct details.**

### Problem

After upgrading to 3.4.0, if the ActiveMatrix Administrator is SSL-enabled, it does not load in the latest browser and the connection cipher suite does not display the following details:

- Signature Algorithm: SHA256WithRSA
- Connection Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

All latest browsers support RSA certificates. Prior to upgrading to ActiveMatrix Service Grid 3.4.0, if the SSL certificate was using DSA then after upgrade, you must update the certificate created using RSA. Update the keystore file used for ActiveMatrix Administrator's HTTP Connector by using the following steps:

### Workaround

1. Select the **Edit TIBCO ActiveMatrix Administrator Server Configuration - V3.4** wizard in the TIBCO Configuration Tool.
2. Select **Edit Http Connection Settings**. The wizard displays the values of the current HTTP connector and its keystores.
3. Update the keystore with new one.
4. Enter the key alias and password.
5. Click **Configure**. The keystore used by the HTTP connector is updated.

### TIBCO Host does not start after downgrading from 3.4.0 to 3.3.1

Make sure the TIBCO JRE is updated after uninstalling ActiveMatrix Service Grid 3.4.0 and points to a version JRE 8 Update 162 or lower.

**In TIBCO ActiveMatrix setup when secure SystemHost and RemoteHosts (Host for which JMX port is secured) are successfully upgraded to TIBCO ActiveMatrix Service Grid 3.4.0, the Administrator UI does not show the updated version of Hosts correctly.**

### Problem

When the Hosts are secured, SystemNode is configured with TLSv1 which is the supported TLS in versions of TIBCO ActiveMatrix prior to 3.4.0. Starting TIBCO ActiveMatrix 3.4.0 TLSv1.2 is supported, and all the Hosts are updated to automatically use TLSv1.2 when upgraded to TIBCO ActiveMatrix 3.4.0, except the Administrator (SystemNode).

### Workaround

When you encounter this issue, run the following command after applying TIBCO ActiveMatrix 3.4.0 Hotfix, or upgrading directly to TIBCO ActiveMatrix 3.4.0 Hotfix, in order to update Administrator (SystemNode) to support TLSv1.2.

Go to `<TIBCO_HOME>/amx/3.4/bin` folder and execute the following command:

```
tibamx_hostmanager updateAdminToTLSv12 -configHomeLocation <TIBCO_CONFIG_HOME>
```



Hosts and Nodes **MUST** be stopped before running the above command. After running the command, restart Administrator (SystemNode).



Above command must be executed only on the machine where SystemNode and SystemNodeReplica (if applicable) is running.

**In TIBCO ActiveMatrix setup when secure SystemHost and RemoteHosts (Host for which JMX port is secured) are successfully downgraded from TIBCO ActiveMatrix Service Grid 3.4.0, the Administrator UI does not show the updated version of Hosts correctly.**

#### Problem

If SystemHost and RemoteHosts JMX ports are secured after upgrading to TIBCO ActiveMatrix 3.4.0, they use TLSv1.2. When this setup is downgraded, RemoteHosts are automatically updated to use TLSv1 since they use JRE 1.7 after downgrade. However, Administrator (SystemNode) still uses TLSv1.2 to connect to RemoteHosts. Therefore Hosts versions is not updated in Administrator UI.

#### Workaround

If you encounter this issue after downgrade, update JRE version of all Hosts to JRE 1.8.

**After upgrading to TIBCO ActiveMatrix 3.4.0 Hotfix, Administrator version is displayed as 3.4.0 instead of 3.4.0.<Hotfix version>**

#### Problem

1. TIBCO ActiveMatrix 3.4.0 is installed (without selecting **TIBCO ActiveMatrix PD Governance** installation profile) to an earlier version of TIBCO ActiveMatrix setup with TIBCO ActiveMatrix Policy Director Governance configured.
2. TIBCO ActiveMatrix 3.4.0 Hotfix is installed in the same `<TIBCO_HOME>`.
3. Upgrade to TIBCO ActiveMatrix 3.4.0 Hotfix fails with the following error:  

```
product feature com.tibco.governance.gws.product.feature:1.2.0 not found in any local machine model
```
4. TIBCO ActiveMatrix 3.4.0 is installed again by selecting only **TIBCO ActiveMatrix PD Governance** installation profile.

Upgrade to TIBCO ActiveMatrix 3.4.0 Hotfix is successful, but Administrator version is displayed as 3.4.0 instead of 3.4.0.<Hotfix version>.

#### Workaround

- If you have installed TIBCO ActiveMatrix Policy Director Governance and already upgraded to TIBCO ActiveMatrix 3.4.0, use the following workaround to apply TIBCO ActiveMatrix 3.4.0 Hotfix:

Run **applyPatch** command to apply TIBCO ActiveMatrix 3.4.0 Hotfix in this case. After running **applyPatch** command Administrator version is displayed as 3.4.0.<Hotfix version>.

- If you have installed TIBCO ActiveMatrix Policy Director Governance and not upgraded to TIBCO ActiveMatrix 3.4.0 Hotfix then use Workaround A or Workaround B to upgrade to TIBCO ActiveMatrix 3.4.0 Hotfix:

#### Workaround A

1. Install TIBCO ActiveMatrix 3.4.0 Hotfix again.
2. Upgrade using TIBCO Configuration Tool (TCT).

**Workaround B**

1. Navigate to *TIBCO\_HOME*\amx\<version>\scripts\upgrade and edit `tct-upgrade.properties` file.
2. Change the property values as follows:  

```
amx.platform.patch.version=3.4.0.<Hotfix version>  
amx.node.upgrade.version=3.4.1
```
3. Upgrade using TIBCO Configuration Tool (TCT).

# Uninstallation

Uninstall TIBCO products using the TIBCO Universal Installer. The installer runs on multiple platforms. You can run the installer in the GUI mode or console mode.

Using the installer, you can uninstall all products in a particular *TIBCO\_HOME*, or you can uninstall specific products that have been installed in a *TIBCO\_HOME*.

## Prerequisites for Uninstalling

### Procedure

1. Shut down all running TIBCO applications.
2. If a product is started as a Windows Service, make sure it is stopped gracefully and there are no open connections to servers such as the Service Performance Manager server and the Enterprise Message Service server.
3. If you want to uninstall TIBCO Implementation Type for TIBCO Adapters, follow these steps before you uninstall the product.
  - a) From the Administrator GUI, undeploy and delete all applications that were deployed from EAR files.
  - b) From the System folder of the deployed applications, undeploy and delete the `com.tibco.amx.it.proxy.apl` application.
  - c) In the Administrator GUI, select **Software Management > Application Templates** and delete TIBCO Proxy Implementation Type Application Template.
  - d) In the TIBCO Administrator GUI, select **Admin Configuration > Plug-ins** and undeploy and delete the TIBCO Implementation Type for the TIBCO Adapters plugin.
  - e) Stop the TIBCO Host and Administrator server processes.

## Uninstalling in GUI Mode

1. Run *TIBCO\_HOME/tools/universal\_installer/TIBCOUniversalInstaller*.
2. Select the **Uninstall Products From Selected TIBCO Home Location**.
3. Select the *TIBCO\_HOME* location from the **TIBCO Home Location** drop-down list.  
The Welcome dialog appears. Click **Next**.
4. Select an uninstallation option:
  - **Custom Uninstall:** You can select the products to be removed.
  - **Typical Uninstall:** The universal uninstaller removes all the products in this *TIBCO\_HOME*.
5. Click **Next**.
6. If you selected the **Custom Uninstall (Select The Products To Be Removed)**:
  - a. Select the products to be uninstalled.



Starting with 3.4.0, TIBCO ActiveMatrix Policy Director Governance and TIBCO ActiveMatrix Service Performance Manager are a part of TIBCO ActiveMatrix Service Grid. So, you can only select TIBCO ActiveMatrix Service Grid for uninstallation. You cannot select TIBCO ActiveMatrix Policy Director Governance and TIBCO ActiveMatrix Service Performance Manager separately.

- b. Click **Uninstall**.

7. Review the **Pre-Uninstall Summary** and click **Uninstall** to start the uninstallation process.
8. Review the **Post-Uninstall Summary** and click the **Finish** button to exit the uninstall wizard.

## Uninstalling in Console Mode

Uninstalling in the console mode helps you uninstall from the command line.

### Procedure

1. Using a command window, navigate to the `TIBCO_HOME/tools/universal_installer` directory.
2. Type the following command at the command prompt:  
`TIBCOUniversalInstaller -console`
3. Complete the uninstallation by responding to the console window prompts.



Starting with 3.4.0, TIBCO ActiveMatrix Policy Director Governance and TIBCO ActiveMatrix Service Performance Manager are a part of TIBCO ActiveMatrix Service Grid. So, you can only select TIBCO ActiveMatrix Service Grid for uninstallation. You cannot select TIBCO ActiveMatrix Policy Director Governance and TIBCO ActiveMatrix Service Performance Manager separately.