



TIBCO iProcess® Engine

Configuration Guide for Cloud

Version 11.9.0
August 2022



Contents

Contents	2
Introduction	4
Document Scope	4
Overview	4
Configuring Virtual Machines	6
Configuring an Imported Virtual Machine (RHEL)	6
Configuring an Amazon Machine Image or Azure Virtual Machine	8
Configuring Security Groups	10
Examples of Security Groups for TIBCO iProcess Engine on AWS	10
Configuring Security Groups When iProcess Workspace (Windows) Is Installed in AWS	10
Configuring Security Groups When iProcess Workspace (Windows) Is Installed on an External Machine	13
Configuring Security Groups When iProcess Workspace (Browser) is used to Connect to iProcess Engine	16
Examples of Security Groups for TIBCO iProcess Engine on Azure	18
Configuring Security Groups When iProcess Workspace (Windows) Is Installed in Azure	18
Configuring Security Groups When iProcess Workspace (Windows) Is Installed on an External Machine	20
Configuring Security Groups When iProcess Workspace (Browser) Is used to Connect to iProcess Engine	22
Configuring Cloud Databases for iProcess Engine	25
Sample Configuration for Oracle Database on Amazon RDS	25
Sample Configuration for SQL Database on Microsoft Azure	27

CORs Filter Configuration	29
Version x.x.x	29
Configuring TIBCO iProcess Technology Plug-ins	30
Setting Parameters	30
Support for EAICOM	31
Related Documents	32
Known Issue	34
Troubleshooting	35
Authentication Error	35
TIBCO Documentation and Support Services	37
Legal and Third-Party Notices	39

Introduction

This guide describes how to set up TIBCO iProcess® Engine and the related components on the cloud.

Document Scope

This guide explains how to set up the following products on Amazon Web Services (AWS) and Microsoft Azure:

- TIBCO iProcess® Engine
- TIBCO iProcess® Workspace (Windows)
- TIBCO iProcess® Workspace (Browser)
- TIBCO iProcess® Workspace Plug-ins
- TIBCO iProcess® Technology Plug-ins

In addition, it also provides examples to illustrate how iProcess Engine, database servers, and one or multiple of the following components communicate with each other on the cloud environment.

The examples in this guide explain how these products can operate in some commonly used environments. Some of the examples include environments that are a combination of different platforms and database types.



Note

The concepts explained and applied in the example scenarios can be extended to set up iProcess Engine for Cloud on other less common environments.

Overview

TIBCO iProcess Engine can be configured for Amazon Web Services (AWS) or Microsoft Azure by performing tasks listed in the following sections:

1. [Configuring Virtual Machines](#)
2. [Configuring Security Groups](#)
3. [Configuring TIBCO iProcess Technology Plug-ins](#)

Configuring Virtual Machines

This section explains how to configure a virtual machine (VM) so that iProcess Engine, database server, and other associated components function correctly. You can configure an imported Red Hat Enterprise Linux (RHEL) virtual machine image or create a new virtual machine on your respective cloud service. For example, you can create an Amazon Machine Image (AMI) on AWS or an Azure Virtual Machine on Microsoft Azure.

Configuring an Imported Virtual Machine (RHEL)

You can configure values for an imported virtual machine (VM) in AWS and Azure for it to function correctly.

Prerequisites

Before you can configure a VM, you must perform the following steps:

1. Import a VM. For more information, see [VM Import/Export](#) for AWS or [Import/Export Services](#) for Azure.
2. Start the instance on which you imported the VM for iProcess Engine and the database server. See [Launch Your Instance](#) on the AWS or [Virtual Machines Documentation](#) for Azure.

Procedure

1. Turn off the firewall for all created instances.
2. In the database server files, update the private IP of your domain on the instance where you imported iProcess Engine. For example, for an Oracle Database Server, update `tnsnames.ora` and `listener.ora` files.
3. When you import a virtual machine in AWS or Azure, it is assigned a dynamic

machine name. However, iProcess Engine still has the old machine name entry because of which it cannot be recognized by the connected peripherals or applications.

To fix this, correct the machine name for node entry in `swpro.node_cluster` table. You can use one of the following options to change the machine name:

- Run the following command:
`UPDATE swpro.node_cluster SET physical_machine_name='ip-192-0-2-0'`
`where master=1;`
 where "ip-192-0-2-0" is the hostname of the machine.
 - Run the `hostname` command to get the string to set the correct name here.
4. To avoid machine name mismatch errors, remove old machine entries from `/etc/hosts`.
 5. To restrict iProcess Engine processes from accepting incoming RPC requests from within a port range, add a fixed port range by running the following commands. Run the following commands to add a fixed port range:
 - a. `swadm ADD_RANGE -p <port_number> -s <port_range>`
 Example: `swadm ADD_RANGE -p 46000 -s 20`
 - b. `swadm SET_RANGE 1 <port_range_ID>`
 Example: `swadm SET_RANGE 1 1`



Note

You must perform this step if your iProcess Engine is in a firewalled environment.

For more information, see “Administering Firewall Port Ranges” in the *TIBCO iProcess Engine Administrator’s Guide*.

6. (Only for Oracle Database Server) Add an AQ port range by running the following command:

```
swadm ADD_AQ_PORT_RANGE 1 <port_number> <port_range>
```

For example: `swadm ADD_AQ_PORT_RANGE 1 48000 50`

What to do next

After configuring the imported VMs, you must configure security groups for each VM to control inbound and outbound connections. See [Configuring Security Groups](#).

Configuring an Amazon Machine Image or Azure Virtual Machine

The procedure explains how you can configure values for an Amazon Machine Image (AMI) on AWS or Azure Virtual Machine (AVM) on Azure.

Prerequisites

Before you can configure an AMI or an Azure Virtual Machine, perform the following steps:

1. Ensure that you have installed the following software on one or multiple instances (as per your requirement):
 - TIBCO iProcess Engine
 - A database serverFor a list of supported databases, see *TIBCO iProcess Engine Installation for UNIX or Windows*. If you want to configure a relational databases service, such as Amazon RDS or Azure SQL Database, see [Configuring Cloud Databases for iProcess Engine](#).
2. Start all created instances. See [Launch Your Instance](#) for AWS or [Virtual Machines Documentation](#) for Azure.

Procedure

1. Turn off the firewall for all created instances.
2. Add a fixed port range in the iProcess Engine configuration. This step is important when your iProcess Engine is in a firewalled environment. Adding a fixed port range restricts iProcess Engine processes to accept incoming RPC requests from within that port range. For more information, see “Administering Firewall Port Ranges” in *TIBCO iProcess Engine Administrator’s Guide*. Run the following are commands to add a fixed

port range:

a. `swadm ADD_RANGE -p <port_number> -s <port_range>`

Example: `swadm ADD_RANGE -p 46000 -s 20`

b. `swadm SET_RANGE 1 <port_range_ID>`

Example: `swadm SET_RANGE 1 1`

3. *(Only for Oracle Database Server)* Add an AQ port range by using the following command:

`swadm ADD_AQ_PORT_RANGE 1 <port_number> <port_range>`

For example: `swadm ADD_AQ_PORT_RANGE 1 48000 50`

What to do next

After configuring the virtual machine (AMI or AVM), you must configure security groups for each VM to control inbound and outbound connections. See [Configuring Security Groups](#).

Configuring Security Groups

A security group acts as a virtual firewall for your AWS or Azure instance to control inbound and outbound traffic. You can create multiple security groups for access, as required.

In AWS, when you start an instance in a Virtual Private Cloud (VPC), you can assign the instance to a maximum of five security groups. However, in a Virtual Network (VNET) in Azure, there is no limit to the number of security groups to which an Azure Virtual Machine (AVM) can be assigned. Security groups act at the instance level, not the subnet level. Therefore, each instance in your VPC or VNET can be assigned to a different set of security groups. This section provides examples of configuring security groups for iProcess Engine with different database servers.

Examples of Security Groups for TIBCO iProcess Engine on AWS

The following examples describe some common security group configurations. You can also configure security groups as per your security protocols.

Configuring Security Groups When iProcess Workspace (Windows) Is Installed in AWS

To use iProcess® Workspace (Windows) instances in AWS to connect to TIBCO iProcess Engine, perform the following steps to configure security groups.

1. Start an Elastic Compute Cloud (EC2) instance in your Virtual Private Cloud (VPC).
2. Name the created instance as `ec2-OracleServer` and install the Oracle Database Server on this instance.
3. Start a second EC2 instance in your VPC.
4. Name the created instance `ec2-iPE` and install iProcess Engine on this instance.

5. Start a third EC2 instance in your VPC.
6. Name the created instance `ec2-iPWW` and install iProcess Workspace (Windows) on this instance.
7. Now, create security groups for all three EC2 instances.
 - Create security group `sg-OracleServer` for the `ec2-OracleServer` instance.
 - Create security group `sg-iPE` for the `ec2-iPE` instance.
 - Create security group `sg-iPWW` for the `ec2-iPWW` instance.
8. **Configure `sg-OracleServer`**
 - a. Specify a custom TCP rule so only the machines on an external domain can access the Oracle Database Server (The default port is 1521.)
 - b. Specify a rule on `ec2-OracleServer` for iProcess Engine to communicate with the database server.

Type	Protocol	Port Range	Source		Description
Custom TCP Rule	TCP	22	Custom	192.0.2.0/32	SSH to access the VM
All TCP	TCP	0-65535	Custom	sg-iPE	To allow traffic from members of sg-iPE
Oracle Database Server	TCP	1521	Custom	192.0.2.0/32	To access the Oracle database from an external machine

i Note: 192.0.2.0/32 is used as an example IP address. Replace this with your IP address.

9. Configure `sg-iPE`

- a. Specify a rule on `ec2-iPE` for the database server to communicate with iProcess Engine.
- b. Specify a rule on `ec2-iPE` for iProcess Workspace (Windows) to communicate with iProcess Engine.

Type	Protocol	Port	Source		Description
Custom TCP Rule	TCP	22	Custom	192.0.2.0/32	SSH
All TCP	TCP	0-65535	Custom	sg-OracleServer	To allow traffic from members of sg-OracleServer
All TCP	TCP	0-65535	Custom	sg-iPWW	To allow traffic from members of sg-iPWW

i Note: 192.0.2.0/32 is used as an example IP address. Replace this with your own IP address.

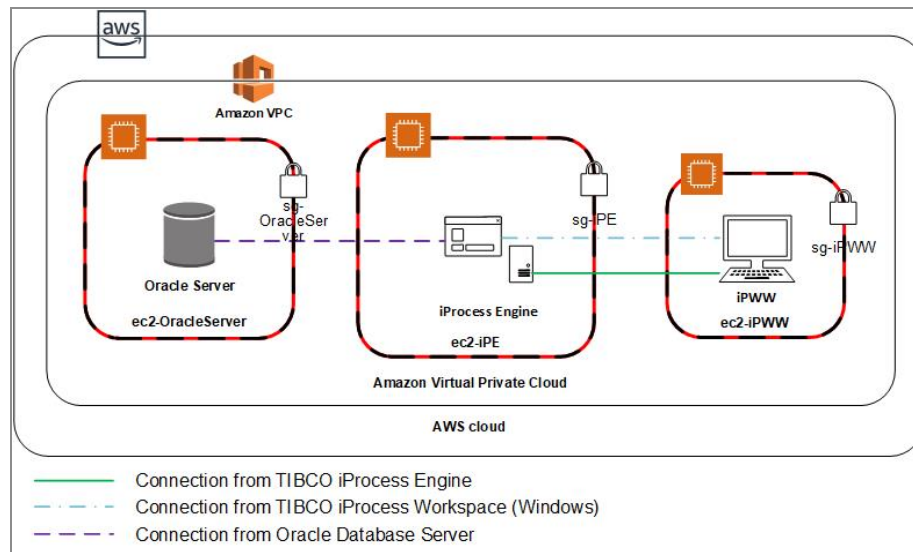
10. Configure sg-iPWW

- Specify a rule on ec2-iPWW for iProcess Engine to communicate with the iProcess Workspace (Windows).
- Specify Remote Desktop (RDP) rule for access to ec2-iPWW from an external domain.

Type	Protocol	Port Range	Source		Description
RDP	TCP	3389	Custom	192.0.2.0/32	Remote Desktop Connection

i Note: 192.0.2.0/32 is used as an example IP address, replace this with your own IP address.

After configuring these security groups, your setup looks something like the following illustration.



Configuring Security Groups When iProcess Workspace (Windows) Is Installed on an External Machine

To connect to iProcess Engine from an external machine that has iProcess Workspace (Windows) installed, perform the following steps to appropriately configure security groups.

1. Start an EC2 instance in your VPC.
2. Name the created instance `ec2-OracleServer` and install the Oracle Database Server on this instance.
3. Start a second EC2 instance in your VPC.
4. Name the created instance `ec2-iPE` and install iProcess Engine on this instance.
5. Install iProcess Workspace (Windows) on the client machine (on an external domain.) For more information, see *TIBCO iProcess Workspace (Windows) Installation* for more information.
6. Now, create security groups for the two EC2 instances:
 - Create `sg-OracleServer` for the `ec2-OracleServer` instance.
 - Create `sg-iPE` for the `ec2-iPE` instance.

7. Configure sg-OracleServer

- a. Specify a custom TCP rule so only machines on an external domain can access the Oracle Database Server (The default port is 1521.)
- b. Specify a rule on ec2-OracleServer for iProcess Engine to communicate with the database server.

Type	Protocol	Port Range	Source		Description
Custom TCP Rule	TCP	22	Custom	192.0.2.0/32	SSH to access the VM
All TCP	TCP	0-65535	Custom	sg-iPE	To allow traffic from members of sg-iPE
Oracle Database Server	TCP	1521	Custom	192.0.2.0/32	To access the Oracle database from an external machine

i Note: 192.0.2.0/32 is used as an example IP address, replace this with your own IP address.

8. Configure sg-iPE

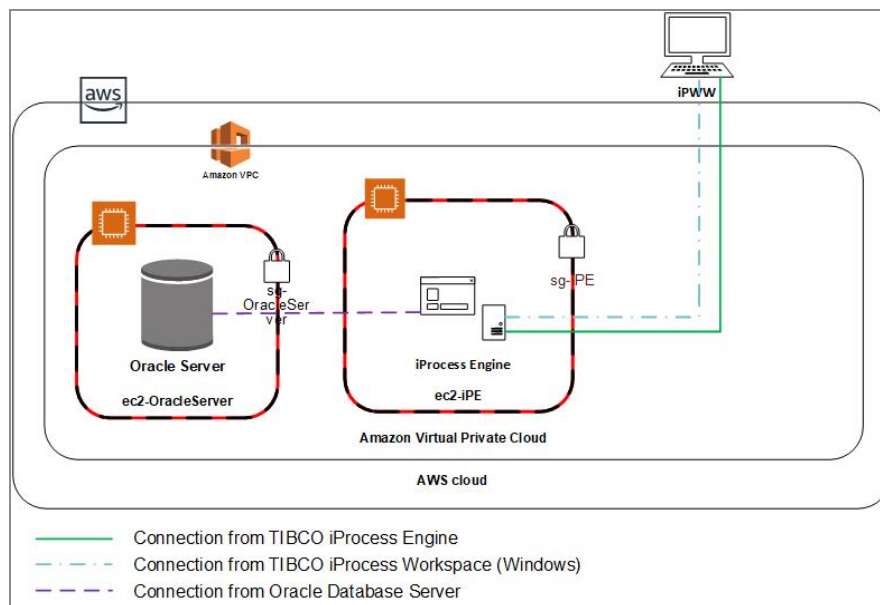
- a. Specify a rule on ec2-iPE for the database server to communicate with iProcess Engine.
- b. Specify a custom TCP rule (for example: 46000-46020) to restrict the number of inbound connections to ec2-iPE.
- c. Specify a custom TCP rule so that only client machines on an external domain can access iProcess Engine on RPC port (The default is 111.)

Type	Protocol	Port Range	Source		Description
Custom TCP Rule	TCP	22	Custom	192.0.2.0/32	SSH to access the VM

Type	Protocol	Port Range	Source		Description
Custom TCP Rule	TCP	46000-46020	Custom	192.0.2.0/32	Port range used by iProcess Engine
All TCP	TCP	0-65535	Custom	sg-OracleServer	To allow traffic from members of sg-OracleServer
Custom TCP Rule	TCP	111	Custom	192.0.2.0/32	To access iProcess Engine

Note: 192.0.2.0/32 is used as an example IP address, replace this with your IP address.

Once you configure these security groups, your setup looks something like the following illustration.



Configuring Security Groups When iProcess Workspace (Browser) is used to Connect to iProcess Engine

To connect to iProcess Engine by using iProcess® Workspace (Browser), perform the following steps to appropriately configure security groups.

1. Start an EC2 instance in your VPC
2. Name the created instance `ec2-OracleServer` and install the Oracle Database Server on this instance.
3. Start a second EC2 instance in your VPC.
4. Name the created instance `ec2-iPETomcat` and install iProcess Engine and iProcess Workspace (Browser) on this instance.
5. Create security groups for the two EC2 instances:
 - Create `sg-OracleServer` for `ec2-OracleServer` instance.
 - Create `sg-iPETomcat` for `ec2-iPETomcat` instance.
6. Configure `sg-OracleServer`
 - a. Specify a custom TCP rule so only machines on an external domain can access the Oracle Database Server (The default port is 1521.)
 - b. Specify a rule on `ec2-OracleServer` for iProcess Engine to communicate with the database server.

Type	Protocol	Port Range	Source		Description
Custom TCP Rule	TCP	22	Custom	192.0.2.0/32	SSH to access the VM
All TCP	TCP	0-65535	Custom	sg-iPE	To allow traffic from members of sg-iPE
Oracle Database Server	TCP	1521	Custom	192.0.2.0/32	To access the Oracle database from an external machine

i Note: 192.0.2.0/32 is used as an example IP address, replace this with your IP address.

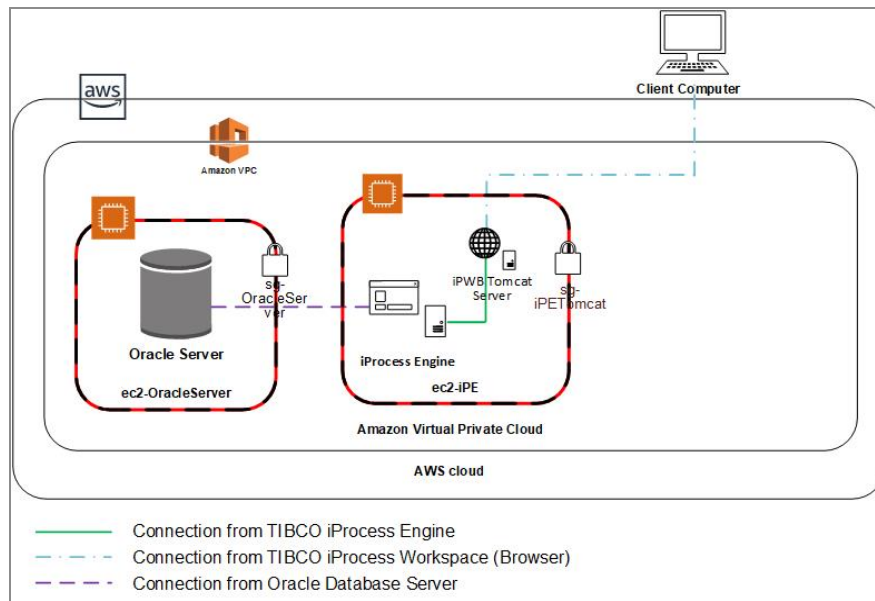
7. Configure sg-iPETomcat

- Specify a rule on ec2-iPETomcat for the database server to communicate with iProcess Engine.
- Specify a custom TCP rule so that only client machines on an external domain can access the iProcess Workspace (Browser) (The default port is 8080.)

Type	Protocol	Port Range	Source		Description
Custom TCP Rule	TCP	22	Custom	192.0.2.0/32	SSH
All TCP	TCP	0-65535	Custom	sg-OracleServer	To allow traffic from members of sg-OracleServer
Custom TCP Rule	TCP	8080	Custom	192.0.2.0/32	Apache Tomcat Server - To connect to iProcess Workspace (Browser)

i Note: 192.0.2.0/32 is used as an example IP address, replace this with your IP address.

Once you configure these security groups, your setup looks something like the following illustration.



Examples of Security Groups for TIBCO iProcess Engine on Azure

The following examples describe some common security group configurations. You can also configure security groups as per your security protocols.

Configuring Security Groups When iProcess Workspace (Windows) Is Installed in Azure

To use iProcess® Workspace (Windows) instances in Azure to connect to TIBCO iProcess Engine, perform the following steps to appropriately configure security groups.

1. Start an Azure Virtual Machine (AVM) in your Virtual Network (VNET).
2. Name the created virtual machine as `avm-OracleServer` and install the Oracle Database Server on this virtual machine.
3. Start a second AVM in your VPC.
4. Name the created virtual machine as `avm-iPE` and install iProcess Engine on this virtual machine.

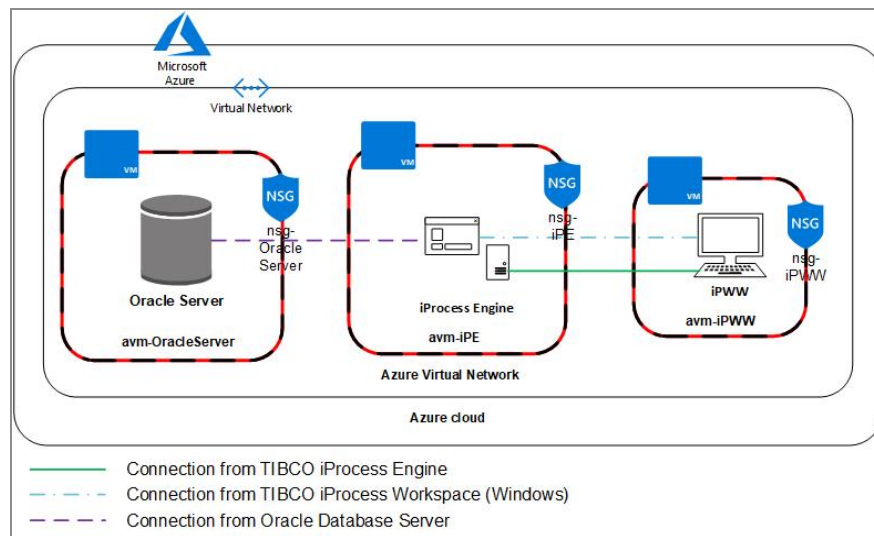
5. Start a third AVM instance in your Virtual Network.
6. Name the created virtual machine as `avm-iPWW` and install iProcess Workspace (Windows) on this virtual machine.
7. Now, create security groups for all three Azure Virtual Machines.
 - Create security group `nsg-OracleServer` for the `avm-OracleServer` instance.
 - Create security group `nsg-iPE` for the `avm-iPE` instance.
 - Create security group `nsg-iPWW` for the `avm-iPWW` instance.
8. **Configure `nsg-OracleServer`, `nsg-iPE`, and `nsg-iPWW`**
 - a. Specify a custom TCP rule that allows only machines on an external domain to access the Oracle Database Server (The default port is 1521.)
 - b. Specify a rule on `avm-OracleServer` for iProcess Engine to communicate with the database server.
 - c. Specify a rule on `avm-iPE` for the database server to communicate with iProcess Engine.
 - d. Specify a rule on `avm-iPE` for iProcess Workspace (Windows) to communicate with iProcess Engine.
 - e. Specify a rule on `avm-iPWW` for iProcess Engine to communicate with the iProcess Workspace (Windows).
 - f. Specify Remote Desktop (RDP) rule for access to `avm-iPWW` from an external domain.

Inbound Security Rules

Priority	Name	Source	Destination	Service	Action
105	iPE_Port	192.0.2.0/32	Any	Custom (Any/111)	Allow
130	Tibco	192.0.2.0/32	Any	Custom (Any/48000-48020)	Allow
180	SPO Port	192.0.2.0/32	Any	Custom (Any/45157)	Allow
1000	default-allow-ssh	192.0.2.0/32	Any	SSH (TCP/22)	Allow

Note: 192.0.2.0/32 is used as an example IP address, replace this with your IP address.

After configuring these security groups, your setup looks something like the following illustration.



Configuring Security Groups When iProcess Workspace (Windows) Is Installed on an External Machine

To connect to iProcess Engine from an external machine that has iProcess Workspace (Windows) installed, perform the following steps to appropriately configure security groups.

1. Start an AVM in your Virtual Network.
2. Name the created virtual machine as `avm-OracleServer`. Install the Oracle Database Server on this virtual machine.
3. Start a second AVM in your Virtual Network.
4. Name the created virtual machine as `avm-iPE`. Install iProcess Engine on this virtual machine.

5. Install iProcess Workspace (Windows) on the client machine (on an external domain). For more information, see *TIBCO iProcess Workspace (Windows) Installation*.
6. Now, create security groups for the two Azure Virtual Machines:
 - Create nsg-OracleServer for the avm-OracleServer instance.
 - Create nsg-iPE for the avm-iPE instance.
7. Configure nsg-OracleServer
 - a. Specify a custom TCP rule that allows only machines on an external domain to access the Oracle Database Server (The default port is 1521.)
 - b. Specify a rule on avm-OracleServer for iProcess Engine to communicate with the database server.
 - c. Specify a rule on avm-iPE for the database server to communicate with the iProcess Engine.
 - d. Specify a custom TCP rule (for example: 46000-46020) to restrict the number of inbound connections to avm-iPE.
 - e. Specify a custom TCP rule that allows only client machines on an external domain to access iProcess Engine on the RPC port (The default is 111.)

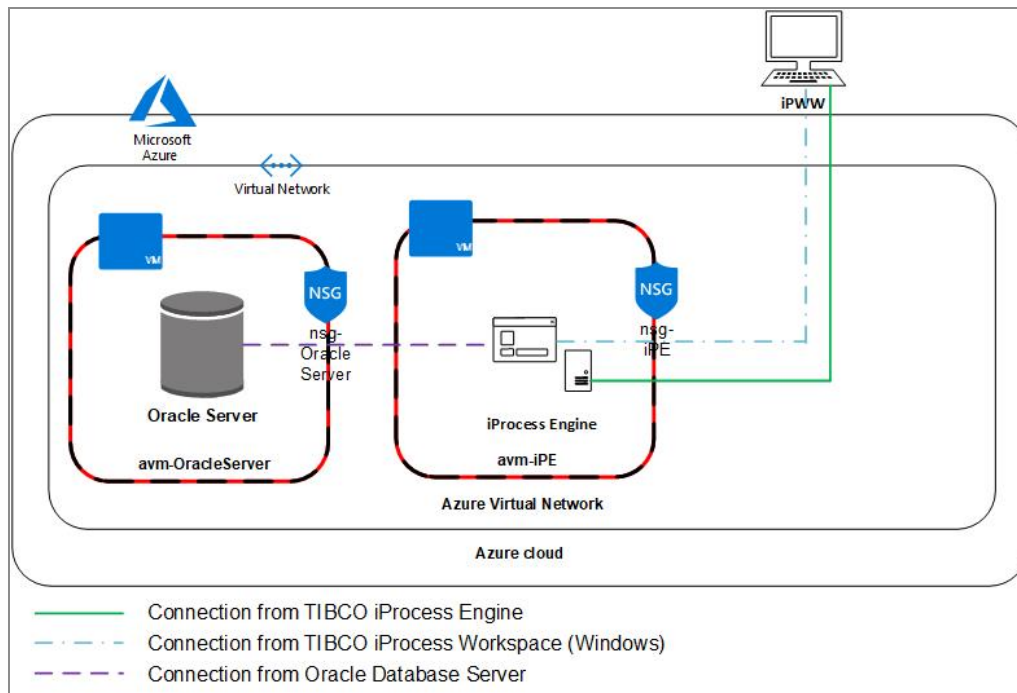
Inbound Security Rules

Priority	Name	Source	Destination	Service	Action
110	Oracle	Any	Any	Custom (Any/1521)	Allow
1000	default-allow-ssh	Any	Any	SSH (TCP/22)	Allow

Outbound Security Rules

Priority	Name	Source	Destination	Service	Action
100	AllTcpOut	Any	Any	Custom (Any/Any)	Allow

After configuring these security groups, your setup looks something like the following illustration.



Configuring Security Groups When iProcess Workspace (Browser) Is used to Connect to iProcess Engine

To connect to iProcess Engine from iProcess® Workspace (Browser), perform the following steps to configure security groups.

1. Start an AVM in your Virtual Network.
2. Name the created virtual machine as `avm-OracleServer`. Install the Oracle Database Server on this virtual machine.
3. Start a second AVM in your Virtual Network.
4. Name the created virtual machine as `avm-iPETomcat`. Install iProcess Engine and iProcess Workspace (Browser) on this virtual machine.
5. Create security groups for the two Azure Virtual Machines:
 - Create `nsg-OracleServer` for `avm-OracleServer` instance.
 - Create `nsg-iPETomcat` for `avm-iPETomcat` instance.

6. Configure nsg-OracleServer

- a. Specify a custom TCP rule so that only machines (on an external domain) can access the Oracle Database Server (The default port is 1521.)
- b. Specify a rule on avm-OracleServer for iProcess Engine to communicate with the database server.
- c. Specify a rule on avm-iPETomcat for the database server to communicate with iProcess Engine.
- d. Specify a custom TCP rule so only client machines on an external domain can access the iProcess Workspace (Browser) (The default port is 8080.)

Inbound Security Rules

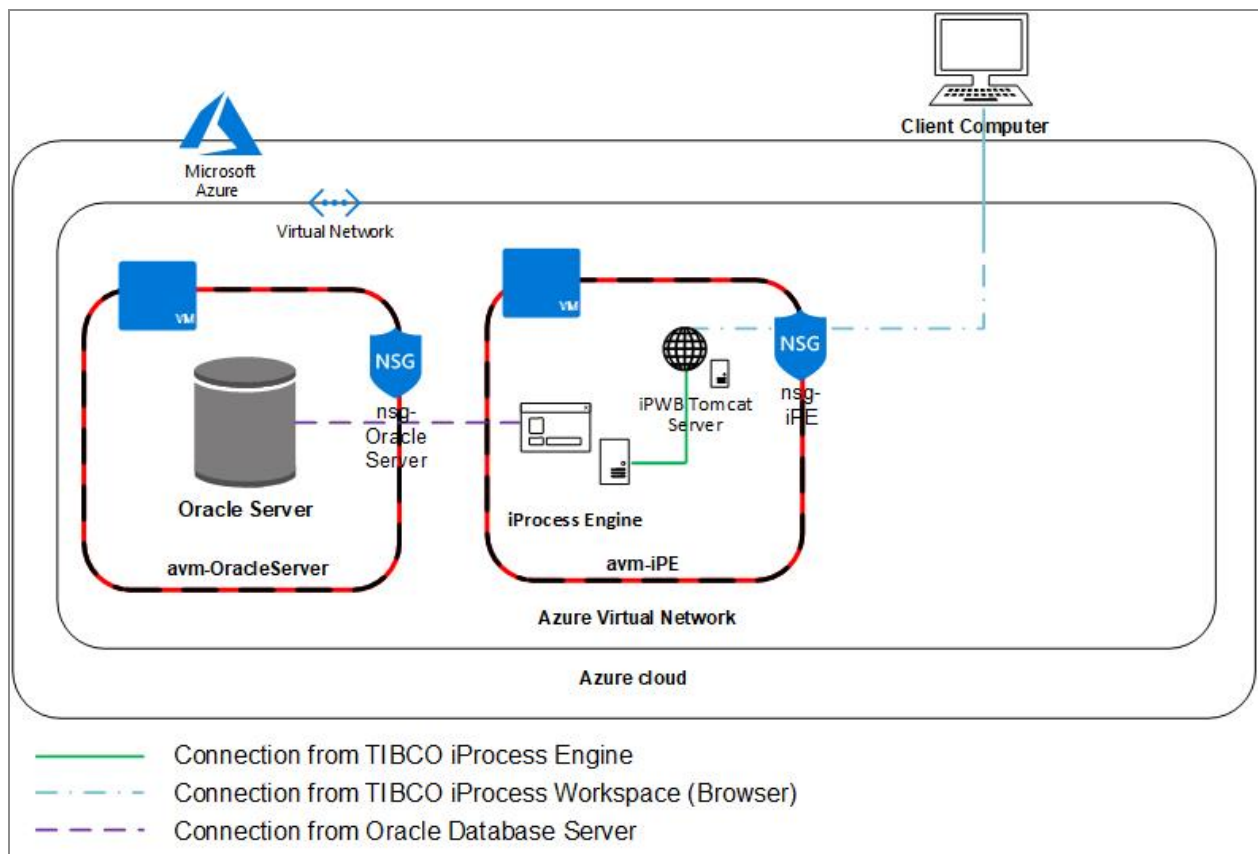
Priority	Name	Source	Destination	Service	Action
200	default-allow-rdp	Any	Any	Custom (TCP/3389)	Allow
300	AllTCP	192.0.2.0/32	Any	Custom (Any/Any)	Allow

Outbound Security Rules

Priority	Name	Source	Destination	Service	Action
100	AllTCP-outbound	Any	Any	Custom (Any/Any)	Allow

i Note: 192.0.2.0/32 is used as an example IP address, replace this with your IP address.

After configuring these security groups, your setup looks something like the following illustration.



Configuring Cloud Databases for iProcess Engine

To use a cloud database, such as Oracle-RDS on AWS or SQL Database on Microsoft Azure, you must configure the same to work with your iProcess Engine setup. This section provides instructions on configuring a cloud database.

Sample Configuration for Oracle Database on Amazon RDS

AWS provides Amazon Relational Database Service (Amazon RDS) that enables you to set up, operate, and scale a relational database on the cloud. Amazon RDS is license-based and works on a “pay only for what you use policy.” For more information about Amazon RDS, visit the Amazon Relational Database Service (RDS) website.

To configure the Oracle database instance on Amazon RDS for connections with iProcess Engine, perform the following steps:

1. Create a database instance on Amazon RDS running Oracle. For more information on how to do this, see the User’s Guide for Amazon Relational Database Service (Amazon RDS).

After selecting the database engine and specifying details for the same (like identifier, password, and so on), the final step is to configure advanced settings for the database, which in this case is Oracle.

2. On the Configure Advanced settings page, add the Oracle database instance to the VPC on which iProcess Engine exists or is to be installed. On this page, you can also define accessibility levels, availability zone, and security groups. The following table lists the fields and their respective values that you must configure on this page.

Database Settings

Field	Required Value
Virtual Private Cloud (VPC)	Select the VPC on which iProcess Engine exists or needs to be installed.
Subnet group	This defines which subnets and IP range the DB instance can use in the selected VPC. You must create a subnet group for the database instance and then select the same in this field. For more information about creating subnets, see User's Guide for Amazon RDS.
Public accessibility	This defines if you want EC2 instances and devices outside the VPC to connect DB instance. If yes, a public IP is assigned to the DB instance.
Availability Zone	This specifies the availability zone of your DB instance.
VPC Security Group	In this field, you can choose an existing security group or create a new one. Security groups have rules authorizing connections from all EC2 instances and devices that must connect to the database instance.

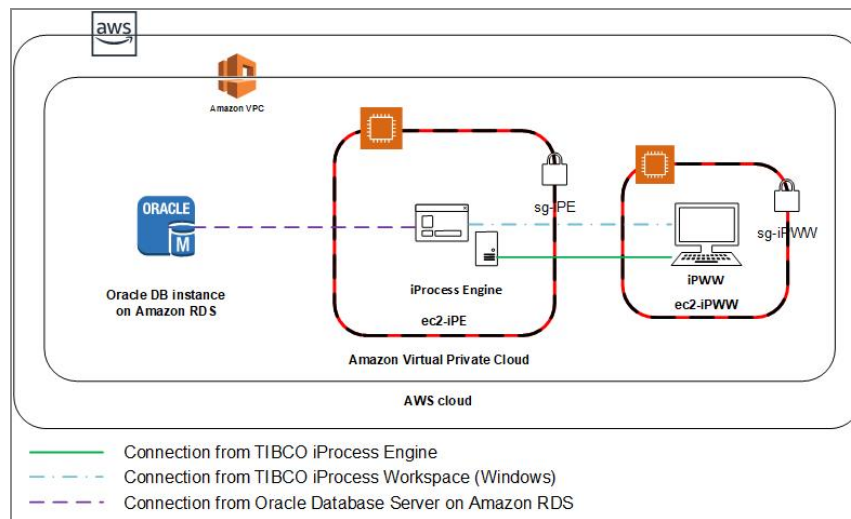
For this sample configuration, the following table lists the security group settings for sg-iPE such that iProcess Engine can connect to the Oracle database instance on Amazon RDS.

VPC Port Range

Type	Protocol	Port Range	Source	Description
All traffic	All	All	192.0.2.0/32	From private network
All traffic	All	All	sg-iPE	From Oracle Database Server on Amazon RDS

i Note: 192.0.2.0/32 is used as an example IP address, replace this with your IP address.

The sample setup would resemble the following illustration.



Sample Configuration for SQL Database on Microsoft Azure

SQL Database is a relational database service provided by Microsoft Azure. It allows efficient migration capabilities from an on-premises SQL Server and is also highly scalable with regards to performance and storage.

For more information about SQL Database, visit the SQL Database page on the Microsoft Azure website.

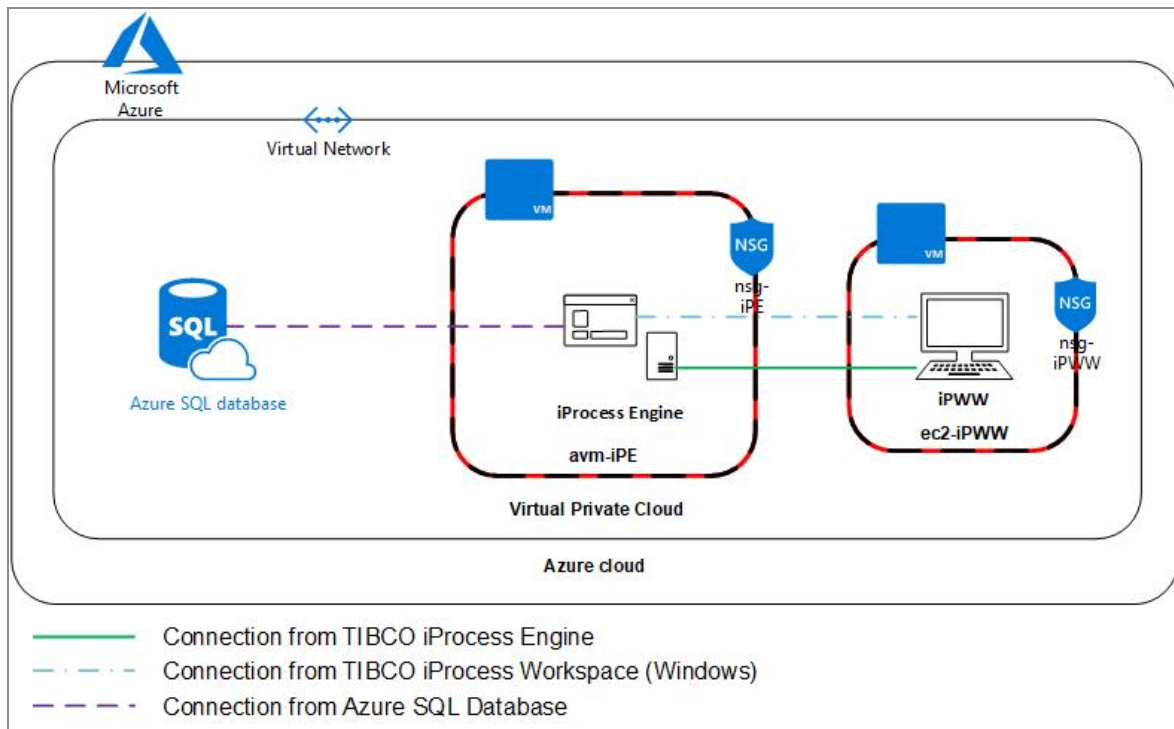
To configure SQL Database on Microsoft Azure for connections to and from iProcess Engine, perform the following steps:

1. From Azure Home, navigate to SQL databases.
2. Select the SQL database that you want to configure with iProcess Engine.
3. Click Firewalls and virtual networks on the left pane.
4. Ensure that **Allow access to Azure services** is ON and the Client IP address is the IP of your private network.

**Note**

If you have iProcess Engine installed on a different virtual network, you must add this to the Azure SQL configuration. For more information, see the documentation for Azure SQL Database.

iProcess Engine can now communicate with Azure SQL Database. See the following illustration.



CORs Filter Configuration

The following functionality and features have been changed in this release of TIBCO iProcess® Engine.

Draft comments: *If no functionality changed, change the short description to "No functionality changes have been made in this release of TIBCO iProcess® Engine".*

Draft comments:

If your product release notes "are" cumulative, change the short description to read "The following features have been changed since the last major release of TIBCO iProcess® Engine". Also, remove the draft comment for the release version subheading.

Version x.x.x

- **Draft comments:** *JIRA-number1*

JIRA summary

- **Draft comments:** *JIRA-number2*

JIRA summary

Configuring TIBCO iProcess Technology Plug-ins

This section describes how to configure iProcess® Technology Plug-ins installed on iProcess Engine.

Setting Parameters

For iProcess Technology Plug-ins to function correctly, you must explicitly set the "java.rmi.server.hostname" property with the public IP of the AWS or Azure machine.

- **Linux/UNIX:** Edit the SWJVM_OPTIONS line in \$SWDIR/eaijava/scripts/env.sh to append
-Djava.rmi.server.hostname=<iProcess Engine FQDN>
- **Windows:** Edit the SWJVM_OPTIONS environment variable to append
-Djava.rmi.server.hostname=<iProcess Engine FQDN>

For example (on both Windows and Linux):

```
SWJVM_OPTIONS="-Dsun.lang.ClassLoader.allowArraySyntax=true -  
Djava.rmi.server.hostname=ec2-52-66-190-210.ap-south-1.compute.amazonaws.com"
```

If you have iProcess Workspace Plug-ins/iProcess Workspace (Browser) installed on a non-AWS or non-Azure network, add the following security group configuration rules to connect to iProcess Engine/iProcess Technology Plug-ins hosted on AWS or Azure.

Type	Protocol	Port Range	Source		Purpose
Custom TCP Port	TCP	10021	Custom	192.0.2.0/32	JMX Port
Custom TCP Port	TCP	10022	Custom	192.0.2.0/32	RMI Port

**Note**

In this table, 192.0.2.0/32 is used as an example IP address, replace this with your IP address.

Support for EAICOM

EAICOM plug-in is not supported in Microsoft Azure. This is because Microsoft Distributed Transaction Coordinator (MSDTC) is not supported on the Azure environment.

Related Documents

This appendix lists documents that you could see in case you need more help.

Document Title	Link or Description
AWS Documentation	https://aws.amazon.com/documentation
Troubleshooting Connecting Instance for AWS	http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesConnecting.html
Amazon RDS Documentation	https://aws.amazon.com/rds/resources/
Azure Documentation	https://docs.microsoft.com/en-us/azure/
Azure SQL Database Documentation	https://docs.microsoft.com/en-us/azure/sql-database/
Troubleshooting Connecting	https://azure.microsoft.com/en-us/resources/knowledge-center/

Document Title	Link or Description
Instance for Azure	

Known Issue

The following issue exists in this release of TIBCO iProcess® Engine.

Key	Summary
IPE-5036	The EAICOM feature is not available on iProcess Engine for Azure.

Troubleshooting

This section describes problems you might encounter and the course of action to resolve them.

Authentication Error

Problem

Http failure response for (unknown url): 0 Unknown Error.

Description

While logging into the iProcess Administration Console, sometimes the server returns an authentication error as stated here.

What to do

To resolve this, check and perform the following tasks:

- export NLS_LANG=American_America.AL32UTF8(NLS_CHARACTERSET on database server and the NLS_LANG env should match)
- Update the IP address value of the attribute apiUrl present in the json file at \$SWDIR/tomcat/webapps/ipac/config/ipac.properties.json with the public IP address. If

Given public IP address : 13.126.165.172

Given private IP address : 172.31.17.169

In the \$SWDIR/config/ipac.properties, IP_ADDR must be updated as

IP_ADDR= 172.31.17.169

In \$SWDIR/tomcat/webapps/ipac/config/ipac.properties.json, apiUrl must be updated as

"apiUrl":"https://13.126.165.172:8443/",

- The browser's cache (related to Administrator console) is cleared before opening the Administrator Console Login page.

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

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.

Product-Specific Documentation

Documentation for TIBCO iProcess® Engine is available on the [TIBCO iProcess® Engine Product Documentation](#) page.

To directly access documentation for this product, double-click the following file:

`TIBCO_HOME/release_notes/TIB_ipe_11.9.0_docinfo.html` where `TIBCO_HOME` is the top-level directory in which TIBCO products are installed. On Windows, the default `TIBCO_HOME` is `C:\tibco`. On UNIX systems, the default `TIBCO_HOME` is `/opt/tibco`.

The following documents for this product can be found in the TIBCO Documentation site:

- *TIBCO iProcess® Engine Architecture Guide*
- *TIBCO iProcess® Engine Configuration Guide for Cloud*
- TIBCO iProcess® Engine Administrator's Guides:
 - *TIBCO iProcess® Engine Administrator's Guide*
 - *TIBCO iProcess® Objects Director Administrator's Guide*
 - *TIBCO iProcess® Objects Server Administrator's Guide*
 - *TIBCO iProcess® Engine Administration Console User Guide*
- TIBCO iProcess® Engine Database Administrator's Guides:
 - *TIBCO iProcess® Engine (DB2) Administrator's Guide*

TIBCO iProcess® Engine (Oracle) Administrator's Guide

TIBCO iProcess® Engine (SQL) Administrator's Guide

TIBCO iProcess® swutil and swbatch Reference Guide

- *TIBCO iProcess® Engine System Messages Guide*
- *TIBCO iProcess® User Validation API User Guide*
- *LDAPCONF Utility User Guide*

How to Contact TIBCO Support

Get an overview of [TIBCO Support](#). You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the [TIBCO Support](#) website.
- 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 [TIBCO Support](#) website. If you do not have a user name, you can request one by clicking **Register** on the website.

How to Join TIBCO Community

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

Legal and Third-Party Notices

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

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

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

TIBCO, the TIBCO logo, the TIBCO O logo, ActiveMatrix BusinessWorks, Business Studio, Enterprise Message Service, Hawk, iProcess, 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 Corporation and/or its affiliates.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: <https://scripts.sil.org/OFL>

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

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

This software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the readme file for the availability of this software version on a specific operating system platform.

THIS 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 © 1994-2022. TIBCO Software Inc. All Rights Reserved.