



SIGMA

Installation Guide

TABLE OF CONTENTS

INSTALLATION OVERVIEW	3
Components Diagram.....	3
SIGMA'S SOFTWARE REQUIREMENTS	4
Supported Operating Systems.....	4
Supported Application Servers.....	4
Supported Databases	4
Supported CA Identity Minder and Governance Minder back-ends	5
Supported Single-Sign-On Option	5
Supported Web Clients (Browsers)	5
SIGMA'S HARDWARE REQUIREMENTS.....	6
SIGMA'S NETWORK REQUIREMENTS	7
SIGMA'S DNS REQUIREMENTS	8
SIGMA'S CLUSTER REQUIREMENTS	8
INSTALLING SIGMA ON AN APPLICATION SERVER	9
Installation Overview.....	9
Installation Pre-requisites	9
Installing SIGMA Using The SIGMA Installer.....	10
Installing SIGMA Using a Manual Procedure.....	12
POST INSTALLATION	19
Weblogic Node Server Start Parameters.....	19
IM Environment Validation	19
Import sigma roles and tasks into im environment	19
task configuration in im environment	19
SIGMA AND SINGLE-SIGN-ON (DEPLOYMENT OPTIONS).....	20
Background.....	20
TEWS Security Settings.....	21
CA GM, Sigma and SSO.....	22
APPENDIX A.....	23

INSTALLATION OVERVIEW

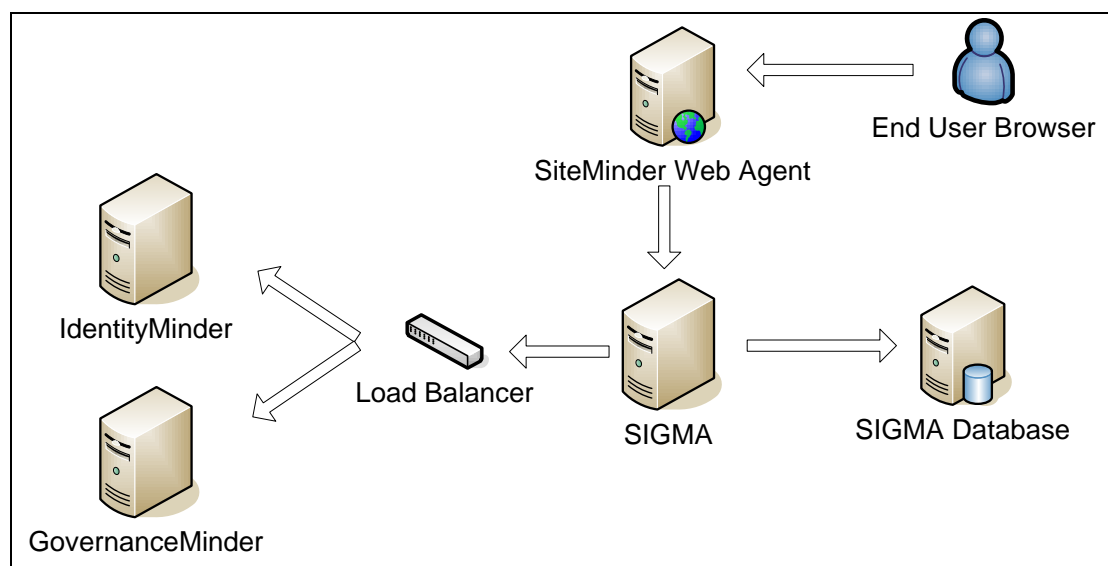
SIGMA is a web-based business-ready identity and access management application, which serves as business logic layer that leverages and aggregates functionality from existing Identity Management products, such as CA IdentityMinder (CA IDM) and GovernanceMinder (CA GM). SIGMA is designed for the non-technical business end user and delivers an intuitive all-inclusive interface in the form of a single page web application.

From a components perspective, SIGMA is a java web application that is deployed on a supported application server or servlet container. SIGMA requires a database for its configuration and persistence stores. SIGMA interfaces with the organization's existing IDM platforms (such as CA IdentityMinder) through SIGMA backend connectors. SIGMA communicates with the IDM backend platforms using the exposed public APIs of these backend systems (for example, Web Services (TEWS) & Workpoint APIs for CA IDM, and web services API for CA GM).

SIGMA can be deployed in a single node configuration or in a multi node cluster configuration. A SIGMA cluster configuration does not depend on the application server cluster abilities and can exist even if the application server itself is not deployed in a cluster mode.

SIGMA can be deployed with basic authentication, where user credentials (user id, password) are validated to a main SIGMA backend connector (for example CA IDM). Alternatively, SIGMA can be integrated with Siteminder to deliver a SSO experience to the end user.

COMPONENTS DIAGRAM



SIGMA'S SOFTWARE REQUIREMENTS

This section describes the software prerequisites for installing SIGMA 3.x. including the supported operating systems, application servers and databases for hosting the SIGMA application server.

SUPPORTED OPERATING SYSTEMS

OS	Version	Notes
Microsoft Windows Server	2008 R2 (SP1,SP2)	64 bit
Red Hat Enterprise Linux	6.x	64 bit

SUPPORTED APPLICATION SERVERS

The following are supported application servers on which SIGMA can be deployed. These servers are supported on all the Operating Systems described above.

Application Server	Version	Java Version	Notes
Apache Tomcat	7.x	Sun JDK 1.6.x update 24 and above	SIGMA Cluster configuration is supported (multiple nodes).
Oracle Weblogic	11g R1 (10.3.5,10.3.6), 12c	Sun JDK 1.6.x update 24 and above.	Native Weblogic Cluster configuration is supported.



General Notes for Supported Application servers:

- Only 64 bit application servers are supported.
- Only Java JDKs are supported. JREs are not supported (SIGMA includes runtime compile elements).

SUPPORTED DATABASES

SIGMA supports the following databases used for its runtime and persistent store.

Vendor	Version	Notes
Oracle	11g R2	RAC is supported.
MySQL	5.5.x	

SUPPORTED CA IDENTITY MINDER AND GOVERNANCE MINDER BACK-ENDS

Vendor	Version	Notes
IdentityMinder	12.5 (SP6-SP15), 12.6 (SP1,SP2)	Supported IDM Application servers: JBOSS, Weblogic, Websphere
Governance Minder	12.5 (SP6 and above) 12.6 (SP0, SP1)	



Note: In case IdentityMinder or GovernanceMinder are deployed in a cluster, a NLB (Network Load Balancer) VIP is required for SIGMA to leverage all IDM/GM cluster nodes.

SUPPORTED SINGLE-SIGN-ON OPTION

Vendor	Version	Notes
SiteMinder	r12.5 r6.0 SP6 CR9 r12.0 SP3 CR11 and above	If SIGMA is integrated with SiteMinder, IDM TEWS must also be integrated with SiteMinder.

SUPPORTED WEB CLIENTS (BROWSERS)

Browser	Version	Notes
Internet Explorer	8,9,10,11,12	On Windows Desktop OS
Mozilla Firefox	3.6 and above	On Windows Desktop OS
Google Chrome	All versions	On Windows Desktop OS
Safari	6.1 and above	On Mac OS



The recommended screen resolution is 1280x800 (pixels)

SIGMA'S HARDWARE REQUIREMENTS

The following are recommended PRODUCTION hardware specifications for the SIGMA application server nodes. For fault tolerance and performance considerations, SIGMA needs to be deployed in at least a 2 node cluster (2 distinct servers).

Component (per node)	Minimum	Recommended
CPU	Dual Core Intel (or compatible) 2.0 GHz Xeon or similar (64 bit)	Quad Core Intel (or compatible) 2.0 GHz Xeon or similar (64 bit)
RAM	16 GB	32 GB
Local Storage	160 GB	160 GB
Database Storage	1GB Initial Size	5 GB Initial Size
Shared Storage (for uploaded files)	50 GB	100 GB

SIGMA'S NETWORK REQUIREMENTS

The following table summarizes the Firewall/Communications requirements between SIGMA and various solution components.

From	To	Port & Protocol	Notes
Web Servers (SM web agents)	SIGMA application Servers	SIGMA Application Server HTTP port	For example: 8080 for Apache Tomcat
SIGMA App Servers	SIGMA Database	Database port	
SIGMA App Servers	IdentityMinder Servers	ALL TCP Ports	HTTP & RMI Traffic
SIGMA App Servers	GovernanceMinder Servers	TCP/8080 (HTTP)	
Identity Minder Servers	SIGMA App Servers	SIGMA Application Server HTTP port	

Note: In case IdentityMinder or GovernanceMinder are deployed in a cluster a NLB (Network Load Balancer) VIP is required for SIGMA to leverage all IDM/GM cluster nodes. SIGMA will be configured to point to the VIP (Virtual IP) representing the CA IDM, CA GM clusters. NLB VIP Characteristics are as follows:

- Relay: all TCP ports.
- Load Balancing Scheme: Round Robin (No ip-stickiness).
- Health Monitor:
 - Basic HTTP on the SIGMA application server HTTP port (for example 8080 on Tomcat).
 - URL to sample: (TBD)
 - Expected string: OK

SIGMA'S DNS REQUIREMENTS

The IDM Application servers FQDN should be resolvable from all the SIGMA Application server nodes. Resolution should be performed either via DNS or a local hosts file override.

SIGMA'S CLUSTER REQUIREMENTS

When SIGMA is deployed in a cluster, SIGMA nodes use Java Groups technology to communicate and replicate configuration and state. SIGMA does this in order to enhance performance and simplify the process of committing/announcing a configuration change to all the nodes in the SIGMA cluster.

This is not a mandatory requirement. In case the requirement is not addressed in a given SIGMA cluster deployment, please see the note at the end of this section for guidelines regarding running SIGMA in such an environment.

Java Groups rely on TCP Multicast. For TCP Multicast to be possible, the SIGMA cluster nodes should reside on the same network switch. In case the SIGMA nodes reside on different network switches, layer 2 Multicast spoofing must be enabled on these switches.

Use the supplied jgroups tester utility to choose and verify that TCP Multicasting is enabled between the servers designated as SIGMA nodes.

1. On each of the SIGMA application servers, navigate to the SIGMA tools folder:
<SIGMA Install Root>\jgroups-multicast-test\
The folder contains a receiver program (jgroups-reciever.bat) and a sender program (jgroups-sender.bat).
2. Run the sender on one node and the receiver on the other.
3. Type something in the sender console and hit enter.
4. The message should display in the receiver console on the other node.
5. Switch receiver and sender sides and try again to validate both directions work.

Note: When the SIGMA cluster requirement, detailed in the section above, is not met, the following should be taken into consideration:

1. After performing configuration changes via the SIGMA Admin UI, you then need to connect

to the SIGMA Admin UI on each node in the cluster and flush (Clear") all the SIGMA caches (using the Tools/Cache section in the Admin UI).

2. Cache based optimization in SIGMA will be available on a per node basis. For example, if a certain user search has been performed on a specific node in the cluster, the result set will be cached only on the node (and not replicated to the other cluster nodes).

INSTALLING SIGMA ON AN APPLICATION SERVER

INSTALLATION OVERVIEW

1. Prepare a database schema and user
2. Install JDK
3. Install Application Server
4. Deploy SIGMA to the application server using the SIGMA installer or a manual procedure
5. Post installation

INSTALLATION PRE-REQUISITES

1 - Install and Prepare a Database

Oracle Database:

1. Install a supported version of the Oracle database. It is recommended that the database will run on a separate server than the SIGMA application server.
2. Create a dedicated schema for SIGMA. The schema user should have the following DB Roles:
 - CONNECT
 - RESOURCE

In addition, the schema user should have a table space quota set (Minimal quota size TBP).

3. Record the database user and password to be supplied to the SIGMA installer.

MySQL Database

1. Install a supported version of the MySQL database.
2. It is recommended that the database will run on a separate server than the SIGMA application server.
3. Create a dedicated database instance for SIGMA. Create a user with all privileges on the SIGMA schema and grant remote access to this user.
4. Record the database user and password to be supplied to the SIGMA installer.

2 - Install JDK

Install a supported Java Development Kit (JDK).

3 - Install the Application Server

1. Install a supported application server.
2. Make sure the application server is configured to run with the JDK you installed.
3. Verify the application server starts correctly.
4. Record the application server base directory to be supplied to the SIGMA installer.

INSTALLING SIGMA USING THE SIGMA INSTALLER

1. Stop the SIGMA application server.
2. Run the SIGMA installer (install.exe) on the computer where the SIGMA application server is installed.
3. Accept the license agreement.
4. Supply the path to the installed JDK home folder.
For example: C:\Program Files\Java\jdk1.6.0_41
5. Select the Application Server type (Tomcat, Weblogic) where SIGMA will be deployed.
In case of Tomcat, enter the Tomcat Windows Service name (as viewed in the windows services mmc snap-in). For example: Tomcat7
6. Choose and enter a UserID and Password to be used as the SIGMA Administrator.
7. Choose a folder location for SIGMA log files.
For example: C:\SIGMA\Logs
8. Select a database type to be used for the SIGMA configuration & runtime store. The installer currently supports MySQL DB only. To install SIGMA on an Oracle database, quit the installer and follow manual installation procedures below.
9. Supply database connection and credential information.
10. Select CA IDM Application server type (JBoss, Weblogic) and IDM version
11. Choose to install the included SIGMA release version or install a patched SIGMA version.
12. Choose a SIGMA home folder (where the tools and documentation will be installed).
13. Review and approve the summary of installation. Click "Install" to perform the actual installation.
14. Validate installation results:
 - a. The application server should have been started by the installer.
 - b. Review application server log file for startup errors.
 - c. Check that the SIGMA Administration UI is up.
 - i. Browse to: <http://<application server host>:port/sigma/admin>
For example: <http://localhost:8080/sigma/admin>
 - ii. Provide the User ID and Password you provided, during installation, for the SIGMA Administrator.
15. For a SIGMA Tomcat cluster installation, rerun this installation procedure on each SIGMA application server node.

16. Go to the Post Installation section.

INSTALLING SIGMA USING A MANUAL PROCEDURE

1. Set application server startup JVM options.
Add the following JVM options to the application server startup:

JVM Option	Notes
-Dsigma.persistence.xml.location=sigma-persistence-oracle.xml	Set only in case Oracle is used a Database for SIGMA.
-XX:MaxPermSize=256m	Needed for runtime compilation of TEWS classes.
-Djava.net.preferIPv4Stack=true -Djgroups.udp.mcast_addr=228.6.7.9 -Djgroups.udp.mcast_port=46656 -Djgroups.bind_addr=<server ipv4 address>	Needed for SIGMA cluster communications. See Cluster Requirements section for more information.
-Dlog4j.logpath=<path to log directory> -Dorg.apache.cxf.Logger=org.apache.cxf.common.logging.Log4jLogger	Designate an operating system path (for example: d:\sigma\logs) to store SIGMA related logs.
-Xms4g -Xmx8g	Minimum and Maximum JVM Heap Memory limits. These values should reflect the expected load and available RAM on the SIGMA server. The example given is for a production server in a large enterprise organization with 32GB of RAM. Memory benchmarks should always be performed and memory prams fine-tuned on regular basis (for example, using JConsole).
-Dhibernate.id.new_generator_mappings=true	Needed for an Oracle Datastore.
-Dlog4j.configuration=file:D:\SIGMA\conf\log4j.properties	Path to the SIGMA log properties file. Use this if you want to override the default log properties. A sample log4j.properties file is included with the install media under the "samples" directory.
-Dsigma.infinispan.configuration.location=file:D:\SIGMA\conf\infinispan-config.xml	Path to the SIGMA caching properties file. Use this if you want to override the default caching properties. A sample infinispan-config.xml file is included with the install media under the

"samples" directory.

For a Weblogic application server, use the Weblogic Administration Console to add these JVM options to each node "Server Start" section.

For Apache Tomcat, use the tomcat monitor utility or startup script (for Linux based deployments), to add these JVM options.

Add the following JVM parameters when using bitronix with Tomcat:

JVM Option	Notes
-Dbtm.root=<Tomcat Home Path> -Dbitronix.tm.configuration=<Tomcat Home Path>\conf\btm-config.properties	Set when bitronix is used with tomcat, make sure you use short names on the Tomcat Home Path

Installing BITRONIX (JTA) on Tomcat

Tomcat application server does not supply JTA transaction Manager functionality that are necessary for SIGMA. We recommend using Bitronix which is an open-source JTA transaction Manager. Bitronix source code can be found in <http://docs.codehaus.org/display/BTM/Download>.

- Copy to following jar from the Bitronix distribution to your Tomcat lib folder
 - slf4j-api.jar
 - slf4j-jdk14.jar
 - jta_1.1.jar
 - btm-tomcat55-lifecycle.jar
 - btm.jar
- Create a file in the tomcat configuration folder called *resources.properties* with the following configuration:


```
resource.ds.className=com.mysql.jdbc.jdbc2.optional.MysqlXADataSource
resource.ds.uniqueName=jdbc/acpdb
resource.ds.minPoolSize=10
resource.ds.maxPoolSize=10
resource.ds.driverProperties.URL=jdbc:mysql://10.0.0.70/sigma-14
resource.ds.driverProperties.user=sigma
resource.ds.driverProperties.password=Giraffe1
resource.ds.allowLocalTransactions=true
resource.ds.driverProperties.pinGlobalTxToPhysicalConnection=true
```

- Edit the resources.properties file *resource.ds.driverProperties.URL* parameter with your schema parameters.

4. Create a file in tomcat configuration folder called `btm-config.properties` with the following configuration:

```
bitronix.tm.serverId=tomcat-btm-node0
```

```
bitronix.tm.journal.disk.logPart1Filename=${btm.root}/work/btm1.tlog
```

```
bitronix.tm.journal.disk.logPart2Filename=${btm.root}/work/btm2.tlog
```

```
bitronix.tm.resource.configuration=${btm.root}/conf/resources.properties
```

5. Edit `server.xml` file in Tomcat conf directory, under the line
`<Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"/>`

Add this line

```
<Listener className="bitronix.tm.integration.tomcat55.BTMLifecycleListener"/>
```

6. Edit `Context.xml` file in Tomcat conf directory, under the line
`<WatchedResource>WEB-INF/web.xml</WatchedResource>`

Add this line

```
<Transaction factory="bitronix.tm.BitronixUserTransactionObjectFactory" />
```

```
<Resource name="jdbc/acpdb" auth="Container" type="javax.sql.DataSource"
```

```
factory="bitronix.tm.resource.ResourceObjectFactory" uniqueName="jdbc/acpdb"/>
```

```
<Resource name="TransactionSynchronizationRegistry" auth="Container"
```

```
type="javax.transaction.TransactionSynchronizationRegistry"
```

```
factory="bitronix.tm.BitronixTransactionSynchronizationRegistryObjectFactory"/>
```

2. Create a database data source in the Application server to connect to the SIGMA database.

- a. Data source JNDI Name: `jdbc/acpdb`

Example 1: on Weblogic using a MySQL database:

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains a 'Domain Structure' tree with 'Services' expanded, showing 'Data Sources'. Below it is a 'How do I...' section with links to create JDBC data sources. The main area shows the 'Settings for jdbc/acpdb-mysql' configuration page. The 'General' tab is selected, showing the 'Name' as 'jdbc/acpdb-mysql' and the 'JNDI Name' as 'jdbc/acpdb'. There are checkboxes for 'Row Prefetch Enabled' and 'Stream Chunk Size' set to 256.

The screenshot shows the WebLogic console interface. At the top, there is a navigation bar with links: Home, Log Out, Preferences, Record, and Help. Below this is a breadcrumb trail: Home > Summary of Servers > ManagedServer_Local > Summary of JDBC Data Sources > jdbc/acpdb-mysql > Summary of Sources > jdbc/acpdb-mysql. The main title is 'Settings for jdbc/acpdb-mysql'. There are several tabs: Configuration, Targets, Monitoring, Control, Security, and Notes. Under the 'Configuration' tab, there are sub-tabs: General, Connection Pool (selected), Transaction, Diagnostics, and Identity Options. A 'Save' button is located at the top left of the configuration area. Below the tabs, there is a descriptive text: 'The connection pool within a JDBC data source contains a group of JDBC connections that applications request. Connections within it are created when the connection pool is registered, usually when starting up WebLogic. Use this page to define the configuration for this data source's connection pool.' The configuration fields are as follows:

- URL:** jdbc:mysql://10.0.0.70:3306/sigmacc
- Driver Class Name:** com.mysql.jdbc.Driver
- Properties:** A text area containing 'user=sigma'.
- System Properties:** An empty text area.

Example 2: Apache Tomcat and an Oracle database:

Context.xml file should contain the following definition:

```
<Resource maxWait="10000" maxIdle="30" maxActive="100" password="secret" username="sigma"
url="jdbc:mysql://10.0.0.70/sigma_schema?autoReconnect=true" driverClassName="com.mysql.jdbc.Driver"
type="javax.sql.DataSource" auth="Container" name="jdbc/acpdb"/>
```

Example 3: Apache Tomcat and a MySQL database:

Context.xml file should contain the following definition:

```
<Resource name="jdbc/acpdb" auth="Container" type="javax.sql.DataSource"
driverClassName="com.mysql.jdbc.Driver" url="jdbc:mysql://10.0.0.70:3306/sigma-schema" username="sigma"
password="secret" testOnBorrow="true" validationQuery="SELECT 1" maxActive="100" maxIdle="30"
maxWait="10000" />
```

Note: `testOnBorrow="true"` and `validationQuery="SELECT 1"` are mandatory properties for MySQL.

3. Copy relevant CA IDM client JARs to the SIGMA application server lib folder.

- a. Locate the Workpoint Designer home folder on your IDM deployment server:
For example:

C:\CA\Identity Manager\IAM Suite\Identity Manager\tools\Workpoint\

- b. Copy the following JAR file from the <workpoint designer home>\lib folder to the application server \lib folder:

- wpCommon.jar
- wpClient.jar

In case IM is installed on JBoss also copy:

- jbossall-client.jar

In case IM is installed on Weblogic also copy:

- Wlclient.jar

Destination \lib folder depends on the SIGMA application server.

For Apache Tomcat:

<tomcat home>\lib

For example:

C:\tomcat7\lib

For Weblogic

<Weblogic server home>\server\lib

For example:

D:\Oracle\Middleware\wlserver_10.3\server\lib

4. Deploy the SIGMA application war (sigma-<version info>.war) to the application server.

a. For Apache Tomcat:

- i. Stop the application server
- ii. Copy the sigma war file to the tomcat webapps folder:

<tomcat home>\webapps

For example:

C:\tomcat7\webapps\

iii. Start the application server

b. For Weblogic:

- iv. Use the Weblogic Administration Console to deploy the sigma war as a web application.
- v. (TBD)

5. Create an application server user and group for protecting the SIGMA Admin UI.

To access the SIGMA Admin UI you need to create the appropriate security group and users in the application server.

For Weblogic

- a. Using the Weblogic Admin Console, create a Weblogic security group called "SigmaAdmins".
- b. Create a user called "sigma" or any other user and place that user in the "SigmaAdmins" group.

The first screenshot shows the 'Settings for myrealm' page, specifically the 'Groups' tab. A table lists various groups, with 'SigmaAdmins' highlighted. The second screenshot shows the 'Users' tab, where the 'sigma' user is highlighted. The third screenshot shows the 'Groups' tab for the 'sigma' user, where 'SigmaAdmins' is selected as a parent group.

Settings for myrealm - Groups

Name	Description	Provider
AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
AppTesters	AppTesters group.	DefaultAuthenticator
CrossDomainConnectors	CrossDomainConnectors can make inter-domain calls from foreign domains.	DefaultAuthenticator
Deployers	Deployers can view all resource attributes and deploy applications.	DefaultAuthenticator
Monitors	Monitors can view and modify all resource attributes and perform operations not restricted by roles.	DefaultAuthenticator
Operators	Operators can view and modify all resource attributes and perform server lifecycle operations.	DefaultAuthenticator
OracleSystemGroup	Oracle application software system group.	DefaultAuthenticator
SigmaAdmins	Sigma Administrators	DefaultAuthenticator

Settings for myrealm - Users

Name	Description	Provider
OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
sigma	Sigma Administrator	DefaultAuthenticator
weblogic	This user is the default administrator.	DefaultAuthenticator

Settings for sigma - Groups

Available:

- AdminChannelUsers
- Administrators
- AppTesters
- CrossDomainConnectors
- Deployers
- Monitors
- Operators
- OracleSystemGroup

Chosen:

- SigmaAdmins

For Tomcat

Add the following to "tomcat-users.xml"

```
<role rolename="SigmaAdministrators"/>
<user username="sigma" password="secret123"
roles=" SigmaAdministrators"/>
```

6. Validate installation results:

- Review SIGMA log file for startup errors.
- Check the SIGMA Administration UI is up.

- i. Browse to: `http://<application server host>:port/sigma/admin`
- ii. For example: `http://localhost:8080/sigma/admin`
- iii. Provide the User ID and Password you defined for the SIGMA Administrator

Note: In case the userid and password for the Admin UI fail, reset the password for that application server user in the application server (using the application server native tools).

7. Go to the Post Installation section.
8. After Post installation see the SIGMA Administration Guide for information about configuring SIGMA.

POST INSTALLATION

WEBLOGIC NODE SERVER START PARAMETERS

1. If you installed SIGMA on a Weblogic server, you will need to set SIGMA specific "Server Start" parameters for each of the Weblogic server nodes on which you selected to deploy SIGMA (during the install phase).

To do this follow instructions in Step 1 of the "INSTALLING SIGMA USING A MANUAL PROCEDURE" section of this document.

IM ENVIRONMENT VALIDATION

1. Using the IM Management Console make sure you can export the IM Environment. Save this export as a backup of the environment before proceeding to the next step.

IMPORT SIGMA ROLES AND TASKS INTO IM ENVIRONMENT

1. Locate the SIGMA-CORE-RoleDefinitions.xml file in the folder where you installed SIGMA.
2. Connect to the IM Management Console and import the Role Definitions XML.

TASK CONFIGURATION IN IM ENVIRONMENT

1. Using the IM Management Console under "Environment Advanced Settings - Web Services", Enable Execution for "Web Services".
2. Modify the "View My Work List" task and enable it for web services in the task profile definition screen.

COPYING WORKPOINT CLINET JARS

Copy the following Jars from the CA IM workpoint lib directory to a local directory. This Local folder directory will be referenced once configuring an IM connector in the SIGMA administration UI:

Jboss Server

1. <JBoss IAM.im Deployment Folder>\library\wpClient.jar
2. <JBoss IAM.im Deployment Folder>\library\wpCommon.jar
3. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\jbossall-client.jar
4. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jboss-client.jar
5. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jboss-common-core.jar
6. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jboss-integration.jar

7. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jboss-javaee.jar
8. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jboss-logging-spi.jar
9. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jboss-remoting.jar
10. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jboss-security-spi.jar
11. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jboss-serialization.jar
12. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jboss-sx-client.jar
13. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\jnp-client.jar
14. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\JBoss\policy.jar

Weblogic Server

1. <CA identity base installation dir>\IAM Suite\Identity Manager\tools\workpoint\lib\wlclient.jar
2. <Weblogic iam_im.ear Deployment Folder>\APP-INF\lib\wpClient.jar
3. <Weblogic iam_im.ear Deployment Folder>\APP-INF\lib\wpCommon.jar

WebSphere Server

1. <WAS_SERVER_HOME>\runtimes\com.ibm.ws.ejb.thinclient_7.0.0.jar
2. <WAS_SERVER_HOME>\runtimes\com.ibm.ws.orb_7.0.0.jar
3. From the <WAS_SERVER_HOME>\WebSphere-ear\Identity Manager\WAS_IMr12.ear file fetch the following jars:
 - a. Library\wpCommon.jar
 - b. Library\wpClient.jar

SIGMA AND SINGLE-SIGN-ON (DEPLOYMENT OPTIONS)

BACKGROUND

When *SIGMA* is used by an end user, all actions performed on the user's behalf in IM (via TEWS) need to run in the user's security context in IM. In case *SIGMA* is not protected by a web SSO solution (like Siteminder),

the end user supplies a user ID and password to *SIGMA*. *SIGMA*, in turn, supplies these credentials to TEWS¹, thus running the IM tasks in the user context.

In case *SIGMA* is protected by a web SSO solution, such as Siteminder, the end user's password is unknown to *SIGMA*. All that is known to *SIGMA* is the user ID and hopefully the user's DN in the IM User directory. *SIGMA*, without the user's password, now needs to invoke actions in IM on behalf of this user.

Several SSO scenarios can exist in a customer's environment, but in order for *SIGMA* to support SSO the TEWS security framework **MUST** be configured for Siteminder authentication, and without "Admin Password required" (see Option 1 in Table 1 below). In addition, *SIGMA* must pass the appropriate Siteminder HTTP headers with the TEWS SOAP call in order for TEWS to accept the user context.

The following table lists the most **common** combinations of initial conditions (before *SIGMA* deployment) and the effects of *SIGMA*'s SSO deployment for existing TEWS clients.

Table 1

SIGMA/IM SSO Options (Before SIGMA deployment)

Option	IM	TEWS	SIGMA	Notes
1	SM Protected	SM Protected (No Admin_password)	SM Protected	This is the most desired/least complex initial conditions for a <i>SIGMA</i> SSO deployment. Here the customer's TEWS setup is already configured for <i>SIGMA</i> SSO support.
2	SM Protected	Not used at all	SM Protected	This is next desired/least complex initial conditions for a <i>SIGMA</i> SSO deployment. Here TEWS is not used by anyone or any process (i.e. bulk load) and its configuration for <i>SIGMA</i> will not affect other processes.
3	SM Protected	Admin_Id & Password Protected	SM Protected	In this case, existing customer TEWS clients (like the bulk loader client) will need to migrate from using Admin_ID and password to using SM authentication. Either this or <i>SIGMA</i> will not be SM protected.
4	No SM	Admin_Id & Password Protected	SM Protected	In this case, existing customer TEWS clients (like the bulk loader client) will need to migrate from using Admin_ID and password to using SM authentication. Either this or <i>SIGMA</i> will not be SM protected.
5	SM Protected	SM Protected (Admin_password is also used)	SM Protected	Here the customer's TEWS setup will need to be changed to NOT use Admin_password while still using SM. This might have an effect on existing TEWS clients. Either this or <i>SIGMA</i> can NOT use SSO.

TEWS SECURITY SETTINGS

¹ In this case the TEWS Security properties need to be set to: "Enable admin_id (allow impersonation)" and "Admin Password is required" (See Screenshot 2 in Appendix A).

Set the following properties for TEWS in the IM environment serving *SIGMA* (Either "Basic" or "Other" can be selected²).

Screenshot 1

TEWS settings for SIGMA with SSO

Home > Environments > Sigma > Advanced Settings > Web Services

Web Services Properties

Property	
Enable Execution	<input checked="" type="checkbox"/>
Enable WSDL Generation	<input checked="" type="checkbox"/>
Enable admin_id (allow impersonation)	<input checked="" type="checkbox"/>
Admin password is required	<input type="checkbox"/>
SiteMinder Authentication	<input type="radio"/> (None) <input checked="" type="radio"/> Basic Authentication <input type="radio"/> Other
WSS Username Token (Password Text)	<input type="checkbox"/>
Generate WSDL in WS-I form (Note: your existing TEWS code may need to be modified).	<input type="checkbox"/>

CA GM, SIGMA AND SSO

The GM Web Services do not implement a support for Siteminder authentication (as of 12.5 SP7). The GM Web services security implementation checks the WSS security header (UserNameToken) and authenticates (either to AD/LDAP or the Eurikify configuration). In order for Sigma to support Siteminder SSO with GM as an endpoint the following configuration is required for the GM portal:

1. AD/LDAP authentication MUST be disabled in GM.
2. Siteminder authentication needs to be enabled in GM (otherwise users will be able to access GM with an incorrect password).

² "Basic" means that IM will automatically configure the realm and protection in the SM policy server when the environment is started.


"Other" means, the SM admin will need to configure the protection of TEWS in SM.

APPENDIX A

TEWS settings for SIGMA without SSO

[Home](#) > [Environments](#) > [Sigma](#) > [Advanced Settings](#) > Web Services

Web Services Properties

Property	
Enable Execution	<input checked="" type="checkbox"/>
Enable WSDL Generation	<input checked="" type="checkbox"/>
Enable admin_id (allow impersonation)	<input checked="" type="checkbox"/>
Admin password is required	<input type="checkbox"/>
 SiteMinder Authentication	<input checked="" type="radio"/> (None) <input type="radio"/> Basic Authentication <input type="radio"/> Other
WSS Username Token (Password Text)	<input type="checkbox"/>
Generate WSDL in WS-I form (Note: your existing TEWS code may need to be modified).	<input type="checkbox"/>