CA Identity Governance

Implimentation Guide

12.6.02a

technologies

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Technologies Product References

- This document references the following CA Technologies products:
- CA Identity Governance
- CA Identity Manager
- CA Single Sign On
- CA User Activity Reporting
- CA SDM
- CA IAM Connector Server

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

This section contains the following topics:

Purpose of This Guide

This guide is intended for Administrators who are responsible for the installation of CA Identity Governance software to become more familiar with the product and its capabilities. Administrators are typically well-trained professionals who are familiar with the target organization and its business processes. This guide assumes that the Administrator has had professional training on an application server system and has access to the CA Identity Governance documentation on the CA Support site.

Role-based Access Control (RBAC)

Role Based Access Control (RBAC) is a project of the National Institute of Standards and Technology (NIST) and is intended to create a comprehensive access security model for the structure and operation of enterprise-level organizations in a high technology environment. RBAC has now reached maturity and has been mandated or recommended for implementation by industry regulations worldwide.

In RBAC, users have roles that grant them with permissions to perform defined operations, such as read/write, and permissions on objects, such as computer files. RBAC incorporates the principles of segregation of duties and organizational hierarchy into its model. Segregation of duties prevents a user with a certain job function to serve in another job function at the same time.

Product Overview

CA Identity Governance complements CA Identity Lifecycle Management products with analytical and client tools for Role-Based Access Control (RBAC).

In RBAC, predefined roles codify common resource usage patterns. Often these roles bundle access rights related to specific business tasks and responsibilities. Users are assigned one or more of these roles based on their current duties, allowing access to only the resources they need.

CA Identity Governance supports implementation of RBAC in the enterprise in several ways:

- **Role Discovery:** CA Identity Governance imports data from CA Identity Manager and other provisioning nodes throughout the enterprise. Based on this data, CA Identity Governance provides powerful analytical tools that efficiently discover common usage patterns and construct an optimized role hierarchy that provides most users the resource access they need. The database and role hierarchy are constantly updated based on user, resource, and provisioning information from across the network.
- **Certification:** periodically, managers throughout the enterprise certify their workers' access privileges - by reviewing the roles assigned to them. Similarly, resource owners periodically review the users and roles that link to their resource. In some jurisdictions, these certifications are mandated by law. CA Identity Governance implements these certifications with a workflow.
- **Real-Time Provisioning Support:** provisioning nodes can query CA Identity Governance in real time using a set of web services. These web services suggest role profiles for users, and answer "what if" questions. In addition, CA Identity Governance can export changes to these nodes, creating account templates and other provisioning tools that reflect the best practices of the role hierarchy. In this way, the role hierarchy proactively controls the privileges assigned to users - realizing the promise of role-based access control.

Important Concepts

Sandbox Model

CA Identity Governance implements RBAC standards without affecting an organization's ongoing operations. The product implements the concept of a sandbox to separate product operation from the organization's ongoing security environment (production server). The assumption is that when working with the product, existing access definitions must first be imported into a sandbox. A sandbox is system where CA Identity Governance is installed, and where role discovery and audit activities are performed without affecting current operations of the organization. All work on discovering new or refining existing access definitions is performed in the product environment.

CA Identity Governance defines roles as a group of users that have a common set of entitlements. Users are people or functions: employees, customers, suppliers, representatives, and so on. An entitlement is a specific right of access that may be an operation or object in formal RBAC terms. Thus, an entitlement can be as specific as a particular access right (Read/Write/Execute) to a specific file in a specific file system on a specific system, and it can also be used to provide a model for access to a computer system (such as, a user group on that system). A link is a connection between a user and an entitlement, indicating that this user possesses a specific access right. A role can include a set of users and a set of entitlements, with the semantics being that all users in the user set are allowed access to all entitlements in the entitlement set.

Most of the work is performed within a product configuration file that is automatically created when access data is imported into CA Identity Governance. A configuration is a data structure that holds a snapshot of the definition of users, entitlements, and roles (if already defined) and the relevant relationships (links) between them.

Import

In a typical implementation, the Role Engineer first imports current access data from the security administration server. Source documents would include a users database file, resources database file, roles file (if existing) and possibly one or more files describing the relationship between one or more entities (users, resources, roles). Using a direct communications link to the production server, CA Identity Governance enables the importing of data from many formats including: CSV, SQL, and RACF. CA Identity Governance creates its own CA Identity Governance “configuration” document, which contains the known user, role, and resource information.

Role Discovery

The role discovery process enables the discovery of roles that were not explicitly defined in the source data and the refining of existing roles. CA Identity Governance's role discovery tools include searching for and proposing basic roles, obvious roles, roles that are almost perfect matches of other roles, and identifying role hierarchy. These options contain sub-menus that enable fine-tuning CA Identity Governance's discovery algorithm to adapt it to the specific configuration that is being analyzed. The results of running these CA Identity Governance options are CA Identity Governance's proposals for role definitions. These roles are individually examined to determine their appropriateness and validity for the organization.

Audit

CA Identity Governance's basic auditing tools apply CA Identity Governance's internal logic and built-in algorithms to an existing configuration to analyze and identify many types of non-conformities or suspicions related to users, roles, and resources. The Role Engineer can apply individual tools to analyze a configuration or can run a comprehensive audit. The output of an audit is the AuditCard, which contains a list of all suspicious records and the type of suspicion involved (currently about 50 different types). The AuditCard also contains a built-in mechanism for tracking progress until resolution is achieved.

Policy Compliance

The Policy Compliance module is an additional audit tool that enables formulating a unique set of Business Process Rules (BPR) that represent various constraints on privileges. These rules are formulated independently of a specific CA Identity Governance configuration and can then be applied to different configurations.

Export

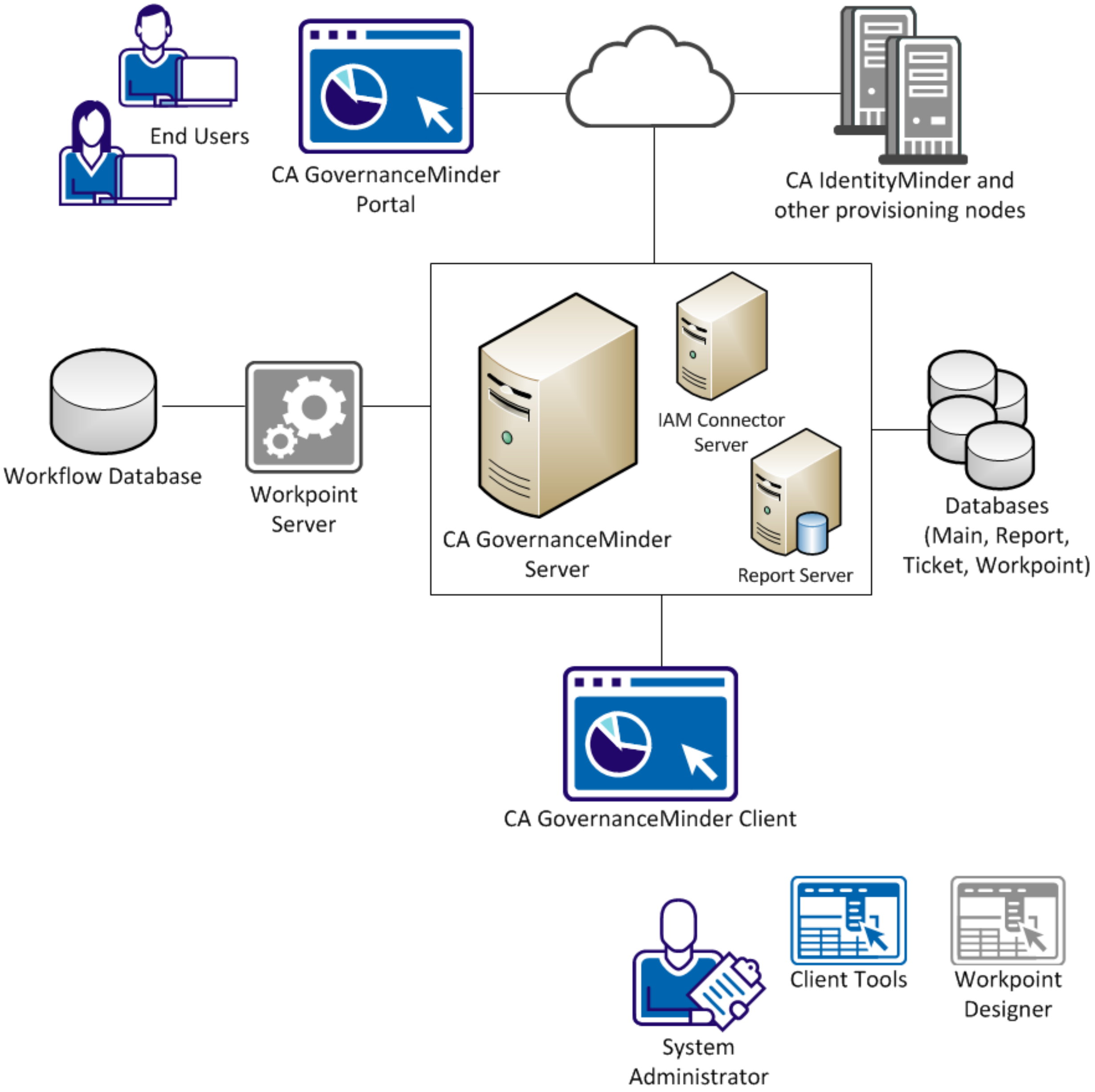
Before uploading a processed CA Identity Governance configuration to the organization's production server, the differences between the original source data and processed CA Identity Governance configuration are examined using a built-in CA Identity Governance option. After verifying the differences and making any necessary changes, the configuration data is directly exported from the CA Identity Governance interface to the production computer's format. The export eliminates cross-platform conversion problems.

Product Components

Every CA Identity Governance implementation includes the following functional components:

- The CA Identity Governance server supports data import, certifications, and the CA Identity Governance web portal and web services.
- CA Identity Governance client tools - let administrators manage data and develop the role hierarchy.
- The Workpoint server application and the Workpoint Designer client support certifications and other CA Identity Governance business processes that are implemented using Workpoint workflows.
- Databases - CA Identity Governance user, role, and resource databases, Workpoint processes, inbox data, and a reporting database.

The following diagram shows the interaction between these components.


End Users
CA GovernanceMinder Portal
CA IdentityMinder and other provisioning nodes
Workflow Database
Workpoint Server
IAM Connector Server
CA GovernanceMinder Server
Report Server
Databases (Main, Report, Ticket, Workpoint)
CA GovernanceMinder Client
System Administrator
Client Tools
Workpoint Designer

The CA Identity Governance server application is the focal point of any CA Identity Governance implementation. It handles various functions and queries, including:

- Automatically importing data from CA Identity Manager and other nodes, and support for web service calls
- Hosting the CA Identity Governance Web Portal
- Conducting certifications and other work flows through the CA Identity Governance Portal, using Workpoint processes and a management system

The Workpoint server application processes workflows such as certifications. Typically a dedicated instance of Workpoint server is installed together with the CA Identity Governance server, but an existing instance can be used.

The role engineer who administers CA Identity Governance uses a set of applications:

- The CA Identity Governance Client Tools manages data import and to define the role-based permissions hierarchy.
- The Workpoint Designer client loads and modifies Workpoint work flows.
- Additional management and configuration functions are exposed to administrators through the CA Identity Governance Portal.

Chapter 2: Planning Your Implementation

This section contains the following topics:

Estimate the Size of your Environment

We recommend the following guidelines to estimate the size of your environment:

Parameter	Small Configuration	Medium Configuration	Large Configuration
Users	5000	40,000	100,000
Roles	80	200	1,500
Resources	500	25,000	50,000
Managers	200	2000	20,000
Total User Links	90,000	2,400,000	4,500,000

Recommended Environment Configurations

We recommend the following configuration guidelines, based on the size of your environment:

	SMALL: Single Virtual Machine	MEDIUM: Single Virtual Machine	LARGE: Distributed, 1 Physical, 1 Virtual Machine

Hardware	■ Memory: 16GB RAM ■ Disk: 100GB ■ CPU: 2 x 2.67GHz	■ Memory: 32GB RAM ■ Disk: 250GB ■ CPU: 2.83GHz	VM1 (GM&WP Servers) ■ Memory: 16GB RAM ■ Disk: 100GB ■ CPU: 2-2.67GHz Physical (DB Server) ■ Memory: 8GB RAM ■ Disk: 150GB ■ CPU: 2 Quad 2.83GHz
Database Parameters	Tablespace datafile: 200MB	■ Memory SGA/PGA: 13GB ■ Tablespace datafile: 200MB ■ Processes: 500 ■ Sessions: 772 ■ ReDo.logfiles: 2GB	Tablespace datafile: 200MB
JVM Values	■ Min=Xms728m ■ Max=Xms8192m	■ Min=Xms728m ■ Max=Xms10240m	VM1: ■ Min=Xms728m ■ Max=Xms8192m

SQL Database Settings

To achieve the best performance, tune the following database settings:

Autogrowth

Set the Autogrowth properties for the all databases, as follows:

- File Growth Percent: 50%
- Maximum File Size: Unrestricted File Growth

Note: For more information about setting the Autogrowth properties, see the documentation for the database that you are using.

Tune the autogrowth property on the following databases:

- WPDS (workflow)
- SDB (eurekify_sdb)
- TicketDB (eurekify_ticketdb)
- ReportDB and I2DB (gvm_datawarehouse)

Maximum threads

Set the maximum worker threads to 12 threads per CPU in the MAX_THREADS setting in the GeneralMonitor.properties file.

The GeneralMonitor.properties file is installed in the following location by default:

gm_install\app_server\\Workpoint

Note: If you performed a new installation, you do not need to modify these settings.

(Optional) After a large data import or purge, you may experience performance degradation. To improve performance, run the dbutil with the '-in' flag on the SDB database. This rebuilds the indexes in the relevant database.

Oracle Database Settings

When using Oracle as the CA Identity Governance database, some tasks may take a long time to complete. To improve the performance when using Oracle, consider the following recommendations:

- Processes: 500
- Session: 500
- REDO.log file size: 2GB each (there are 3)

- Memory: 4GB
- Tablespace datafile, varies as follows:

  TEMP—large amounts of data needs large amounts of temp space. Consider settings as follows:

  - Filesize: 1G
  - Automatically extend datafile, Increment: 200MB
  - Maximum File Size, Value: 20GB

  UNDO:

  - Filesize: 1G
  - Automatically extend datafile, Increment: 200MB
  - Maximum File Size, Value: 20GB

  USERS:

  - Filesize: 1G
  - Automatically extend datafile, Increment: 500MB
  - Maximum File Size: Unlimited

(Optional) When large amounts of data are inserted into the database, run the following statistics commands:

```
execute dbms_stats.gather_schema_stats('${SCHEMA}', DBMS_STATS.AUTO_SAMPLE_SIZE);

alter system flush buffer_cache;

alter system flush shared_pool;
```

Note: Replace *SCHEMA* with the database schema name (username).

Chapter 3: Optimizing CA Identity Governance

This section contains the following topics:

Resize the Memory Cache

When working with large configurations, increase the size of the CA Identity Governance server memory cache. This section describes how to resize the server cache memory.

To resize the memory cache, do the following:

1. Resize the Java virtual machine (JVM) memory heap.
   - JBoss (see page 17)
   - WebSphere (see page 18)
2. Reset the cache limits. (see page 19)

(JBoss) Resize the Java Virtual Machine Memory Heap

To support large configurations, you can expand the Java virtual machine (JVM) memory cache for the CA Identity Governance server.

Follow these steps:

1. Navigate to the following folders on the CA Identity Governance server:

   jboss_install\bin

2. Open the **run.bat** file for editing, and locate the following line:

   ```
   set JAVA_OPTS=%JAVA_OPTS% -Xms728m -Xmx1536m -XX:MaxPermSize=256m
   ```

3. To define the JVM memory heap settings, change the following parameters:

   -Xms

   Defines the minimum size of heap memory. For example, -Xms1200m sets minimum heap memory to 1.2GB. This memory is assigned at server start.

   Note: When using a 64bit JDK, and the available memory is greater than 1400M, set the -Xms parameter to use all available memory.

   -Xmx

   Defines the maximum size of heap memory. For example, -Xmx20g sets maximum heap memory to 20GB. This memory is assigned as needed.

   We recommend, for a 64bit system, that you allocate approximately 3GB of cache memory (RAM) for every 1,000,000 elements allowed in cache memory (3 * maxElementsInMemory (see page 19)).

4. Repeat this procedure on each server in the cluster.

5. Save and close the **run.bat** file.

   The Java virtual machine memory heap has been resized.

(WebSphere) Resize the Java Virtual Machine Memory Heap

To support large configurations, you can expand the Java Virtual Machine (JVM) memory cache for the CA Identity Governance server.

Follow these steps:

1. In the WebSphere Administrative Console, click Servers, Application Servers, and select a server in the cluster.

2. Click Process Definitions, Java Virtual Machine.

3. To define JVM memory heap settings, change the following fields:

   Initial Heap

   Defines the memory reserved for CA Identity Governance upon startup, in megabytes.

   Maximum Heap

   Defines the maximum memory that CA Identity Governance can use, in megabytes.

   We recommend, for a 64bit system, that you allocate approximately 3GB of cache memory (RAM) for every 1,000,000 elements allowed in cache memory (3 * maxElementsInMemory (see page 19)).

4. Repeat this procedure for each server in the cluster.

Reset Cache Limits

To support large configurations, you can expand the cache memory limits.

Cache memory is defined by the number of elements (users, resources, roles, and so on) that can be held in the cache at once. When the cache is full, elements are swapped in and out of memory, which can affect performance. The default setting limits the memory cache to 500,000 elements.

This procedure describes how to reset cache settings for an existing CA Identity Governance implementation. In WebSphere implementations, you can modify these settings before implementation by editing the EAR file you use to install the CA Identity Governance server.

Follow these steps:

1. Edit the **ehcache-sageDal.xml** file on the CA Identity Governance server:

   - For JBoss, this file is found in the following location:

     `jboss_install\server\all\farm\eurekfiy.war\WEB-INF\classes\`

   - For WebSphere, this file is located in the eurekify.ear file found in the following location:

     `/eurekify.war/WEB-INF/classes`

2. In the **defaultCache** entry, change the following attribute:

   maxElementsInMemory

   Defines the maximum number of elements stored in cache memory.

   We recommend that you set this field using the following formula:
   `maxElementsInMemory = total number of entities * 3`

   For example, if you have one universe with 500,000 users and 500,000 roles, set maxElementsInMemory to 3,000,000 elements.

   If you have two universes, each with 500,000 users and 500,000 roles, set maxElementsInMemory to 6,000,000 elements.

3. Save changes to the file and close.

   You have reset cache settings.

Cache Manipulation

Using the server cache improves performance. To improve performance, upload the current Universe and configuration data to the cache. Accessing the server cache is much faster than accessing the hard drives, so users can receive information more quickly when using a cache.

Load Cache

Use this utility to load a specific configuration into the server memory cache.

Follow these steps:

1. In the Portal, go to Administration, Cache, Load Cache.

   The Load Cache screen opens.

2. Select a Configuration from the drop-down list and click OK.

   The information bar indicates that the selected configuration is loaded.

Clear Cache

Use this utility when you update configuration data in the client tools, such as permissions, and you want to be sure that anyone using the system uses the updated data.

Follow these steps:

1. In the Portal, go to Administration, Cache, Clear Cache.

   The Clear Cache screen opens.

2. Click Clear Caches to clear the server memory cache.

   The information bar indicates that the selected configuration is loaded.

(JBoss) Adjusting Portal Session Timeout

The Portal session may cause performance and security issues in your deployment.

You can adjust the default timeout period to work around both issues. Edit the web.xml file to change the Portal session timeout period from the default setting.

Follow these steps:

1. Locate and open the web.xml file located in the following directory:

   gm_home/Server/eurekify-jboss/server/eurekify/deployers/jbossweb.deployer/

2. Locate and change the session configuration section timeout variable:

   ```
   <session-config>
        <session-timeout>30</session-timeout>
    </session-config>
   ```

   Note: The unit of time is minutes.

3. Save changes to the file and close.

How to Prepare an Implementation for Production

We recommend that you perform the following steps before you move CA Identity Governance from a test to a production environment.

1. Mark session cookies as http only. Do the following:

   a. Navigate to the following directory:

   ```
   eurekify-jboss\server\eurekify\deploy\jbossweb.sar
   ```

   b. Open the context.xml file, and add the following line:

   ```
   <SessionCokkie secure="true"httpOnly="true"/>
   ```

   c. Save and close the file.

2. Configure JBoss cross domain policy for Flash. Do the following:

   a. Navigate to the following directory:

   ```
   \eurekify-jboss\server\eurekify\deploy\ROOT.war
   ```

   b. Open the crossdomain.xml file, and replace the default value with the company domain name in the following entry:

   ```
   <allow-access-from domain="*"/>
   ```

   Example: company.com

   c. Save and close the file.

3. Disable HTTP TRACE support in web browsers.Do the following:

   a. Navigate to the following directory:

   ```
   \eurekify-jboss\server\eurekify\deploy\ROOT.war\WEB-INF
   ```

   b. Open the web.xml file, and add the following section:

   ```
   <security-constraint>
                <web-resource-collection>
    <web-resource-name>secure</web-resource-name>
                       <url-pattern>/*</url-pattern>
                       <http-method>GET</http-method>
                       <http-method>POST</http-method>
                       <http-method>HEAD</http-method>
                       <http-method>PUT</http-method>
                       <http-method>DELETE</http-method>
                </web-resource-collection>
          </security-constraint>
   ```

   c. Save and close the file.

4. Configure CA Identity Governance for SSL communication.

   Note: For more information, see the *Installation Guide*.

5. Secure the JBoss JMX Console. Do the following:

   Important! If you do not want to secure the JBoss JMX Console, we recommend that you remove the following files:

   ```
   jmx-console.war, admin-console.war
   ```

   Note: For more information about the JBoss JMX Console refer to the JBoss documentation.

   1. Enable authentication on the JBoss JMX Console. Do the following:

      a. Navigate to the following directory:

      ```
      eurekify-jboss\server\PROFILE\deploy\jmx-console.war\WEB-IN
      F
      ```

      b. Open the web.xml file.

      c. Uncomment the <security-constraint> entry:

      ```
      <security-constraint>
         <web-resource-collection>
            <web-resource-name>HtmlAdaptor</web-resource-name>
            <description>
               An example security config that only allows users with
      the role
               JBossAdmin to access the HTML JMX console web
      application
            </description>
            <url-pattern>/*</url-pattern>
        </web-resource-collection>
        <auth-constraint>
          <role-name>JBossAdmin</role-name>
        </auth-constraint>
      </security-constraint>
      ```

      d. Save and close the file.

2. Enable security domain on the JBoss JMX Console. Do the following:

   a. Navigate to the following directory:

   ```
   eurekify-jboss\server\PROFILE\deploy\jmx-console.war/WEB-IN
   F
   ```

   b. Open the jboss-web.xml file.

   c. Verify that the following section appears:

   ```
   <jboss-web>
     <!-- Uncomment the security-domain to enable security. You
   will
        need to edit the htmladaptor login configuration to setup
   the
        login modules used to authentication users.
     -->
     <security-domain>java:/jaas/jmx-console</security-domain>
   </jboss-web>
   ```

   d. Save and close the file.

3. Enable authentication on the administration console. Do the following:

   a. Navigate to the following directory:

   ```
   eurekify-jboss\server\PROFILE\deploy\management\console-mgr
   .sar\web-console.war\WEB-INF
   ```

   b. Open the web.xml file.

   c. Uncomment the following entry:

   ```
   <security-constraint>
      <web-resource-collection>
         <web-resource-name>HtmlAdaptor</web-resource-name>
         <description>
            An example security config that only allows users with
   the role
            JBossAdmin to access the HTML JMX console web
   application
         </description>
         <url-pattern>/*</url-pattern>
     </web-resource-collection>
     <auth-constraint>
       <role-name>JBossAdmin</role-name>
     </auth-constraint>
   ```

   d. </security-constraint>

a. Save and close the file.

4. Enable security domain on the administration console. Do the following:

   a. Navigate to the following directory:

   ```
   eurekify-jboss\server\PROFILE\deploy\management\console-mgr
   .sar\web.console.war\WEB-INF
   ```

   b. Open the jboss-web.xml file.

   c. Verify that the following entry appears:

   ```
   <jboss-web>
     <!-- Uncomment the security-domain to enable security. You
   will
        need to edit the htmladaptor login configuration to setup
   the
        login modules used to authentication users.
     -->
     <security-domain>java:/jaas/jmx-console</security-domain>
   </jboss-web>
   ```

   d. Save and close the file.