



# API Gateway and Community Manager 7.x Hardening

# Table of Contents

1	Introduction .....	2
2	Deployment Architecture.....	3
2.1	Install Internet-facing and administration applications on separate containers ..	3
2.2	Configure all listeners, internal and external as HTTPS only .....	4
2.3	Configure the Admin console (/admin) on a separate port .....	4
3	Configuration Settings .....	6
3.1	Add the unlimited strength policy to the JDK .....	6
3.2	Configure the product to ignore downstream cookies.....	6
3.3	Configure secure cookies .....	6
3.4	Ignore downstream cookies.....	6
3.5	Disabling SSLv3.....	6
3.6	Restrict the cipher suites used .....	7
3.7	Prevent Forward Proxying .....	7
3.8	Header Propagation in Network Director .....	7
3.9	Header Propagation in Community Manager Subsystem.....	8
3.10	Tune the API Security Credential Cache .....	8
3.11	Configure the Anti-virus Policy to scan for uploaded files.....	8
3.12	Enabling CSRF protection.....	9
3.13	Adding XSS exclusions.....	10
3.14	Turning off User Account Enumeration .....	10
3.15	Configuring Challenge Questions/Answers .....	11
3.16	Disallowing User Profile Modification .....	12
3.17	Configuring Account Login Rules .....	12
3.18	Configuring Password Complexity Rules .....	13
3.19	Configuring X-FRAME-OPTIONS Header .....	13
4	About Akana.....	14

## 1 Introduction

Akana is a recognized leader in API Management and SOA Governance Automation solutions. Our platform-independent solution set includes the API Gateway, which is further broken down into Policy Manager, the centralized administration console, and Network Director, an intermediary that integrates with Policy Manager to provide high-performance, scalable API security and management capabilities. The solution also includes Community Manager, which provides a branded developer portal for the consumption of API by the developer.

This document describes the best practices and configuration settings to harden Akana's API Gateway and Community Manager products. This document is a supplement to Akana's existing "Product Architecture" document showing recommendations for a typical large enterprise.

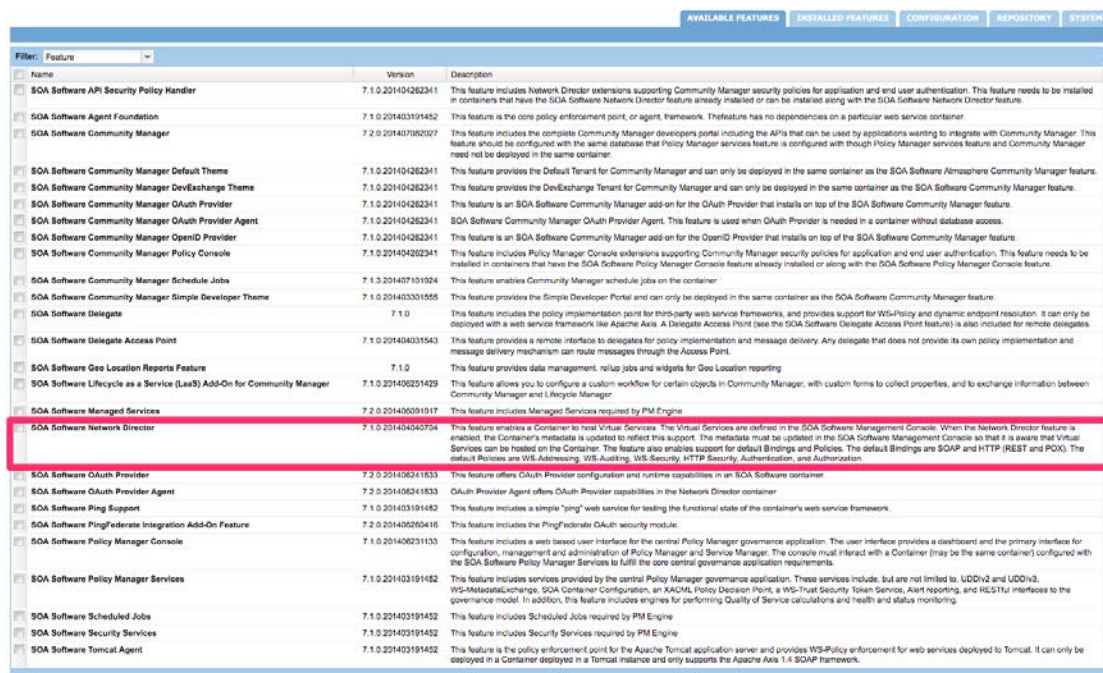
## 2 Deployment Architecture

There are several best practices that cover the deployment of the product in a hardened environment.

An external HSM keystore can be used in place of the out of the box Policy Manager keystore (database). The configuration of Policy Manager with HSM is described in a separate document.

Install Network Director on a separate container

API traffic processing should be handled separately from Web traffic and Admin traffic. To this end, the Network Director should not be installed on the same container as Community Manager, or Policy Manager features:



AVAILABLE FEATURES   <b>INSTALLED FEATURES</b>   CONFIGURATION   REPOSITORY   SYSTEM			
Filter: Feature			
Name	Version	Description	
SOA Software API Security Policy Handler	7.1.0.201404262341	This feature includes Network Director extensions supporting Community Manager security policies for application and end user authentication. This feature needs to be installed in containers that have the SOA Software Network Director feature already installed or can be installed along with the SOA Software Network Director feature.	
SOA Software Agent Foundation	7.1.0.201403191452	This feature is the core policy enforcement point, or agent, framework. This feature has no dependencies on a particular web service container.	
SOA Software Community Manager	7.2.0.201407182027	This feature includes the complete Community Manager developer portal including the APIs that can be used by applications wanting to integrate with Community Manager. This feature should be configured with the same database that Policy Manager services feature is configured with though Policy Manager services feature and Community Manager need not be deployed in the same container.	
SOA Software Community Manager Default Theme	7.1.0.201404262341	This feature provides the Default Tenant for Community Manager and can only be deployed in the same container as the SOA Software Atmosphere Community Manager feature.	
SOA Software Community Manager DevExchange Theme	7.1.0.201404262341	This feature provides the DevExchange Tenant for Community Manager and can only be deployed in the same container as the SOA Software Community Manager feature.	
SOA Software Community Manager OAuth Provider	7.1.0.201404262341	This feature is an SOA Software Community Manager add-on for the OAuth Provider that installs on top of the SOA Software Community Manager feature.	
SOA Software Community Manager OAuth Provider Agent	7.1.0.201404262341	SOA Software Community Manager OAuth Provider Agent. This feature is used when OAuth Provider is needed in a container without database access.	
SOA Software Community Manager OpenID Provider	7.1.0.201404262341	This feature is an SOA Software Community Manager add-on for the OpenID Provider that installs on top of the SOA Software Community Manager feature.	
SOA Software Community Manager Policy Console	7.1.0.201404262341	This feature includes Policy Manager Console extensions supporting Community Manager security policies for application and end user authentication. This feature needs to be installed in containers that have the SOA Software Policy Manager Console feature already installed or along with the SOA Software Policy Manager Console feature.	
SOA Software Community Manager Schedule Jobs	7.1.0.201407101924	This feature enables Community Manager schedule jobs on the container.	
SOA Software Community Manager Simple Developer Theme	7.1.0.201403301555	This feature provides the Simple Developer Portal and can only be deployed in the same container as the SOA Software Community Manager feature.	
SOA Software Delegate	7.1.0	This feature includes the policy implementation point for third-party web service frameworks, and provides support for WS-Policy and dynamic endpoint resolution. It can only be deployed with a web service framework like Apache Axis. A Delegate Access Point (see the SOA Software Delegate Access Point feature) is also included for remote delegates.	
SOA Software Delegate Access Point	7.1.0.201404031543	This feature provides a remote interface to delegates for policy implementation and message delivery. Any delegate that does not provide its own policy implementation and message delivery mechanism can route messages through the Access Point.	
SOA Software Geo Location Reports Feature	7.1.0	This feature provides data management, setup jobs and widgets for Geo Location reporting.	
SOA Software Lifecycle as a Service (LaaS) Add-On for Community Manager	7.1.0.201406251429	This feature allows you to configure a custom workflow for certain objects in Community Manager, with custom forms to collect properties, and to exchange information between Community Manager and Lifecycle Manager.	
SOA Software Managed Services	7.2.0.201406091917	This feature includes Managed Services required by PM Engine.	
<b>SOA Software Network Director</b>	<b>7.1.0.201404042704</b>	<b>This feature enables a Container to host Virtual Services. The Virtual Services are defined in the SOA Software Management Console. When the Network Director feature is enabled, the Container's metadata is updated to reflect this support. The metadata must be updated in the SOA Software Management Console so that it is aware that Virtual Services can be hosted on the Container. The feature also enables support for default Bindings and Policies. The default Bindings are SOAP and HTTP (REST and POX). The default Policies are WS-Addressing, WS-Authorization, WS-Security, HTTP Security, Authentication, and Authorization.</b>	
SOA Software OAuth Provider	7.2.0.201406241833	This feature offers OAuth Provider configuration and runtime capabilities in an SOA Software container.	
SOA Software OAuth Provider Agent	7.2.0.201406241833	OAuth Provider Agent offers OAuth Provider capabilities in the Network Director container.	
SOA Software Ping Support	7.1.0.201403191452	This feature includes a simple "ping" web service for testing the functional state of the container's web service framework.	
SOA Software PingFederate Integration Add-On Feature	7.2.0.201406260416	This feature includes the PingFederate OAuth security module.	
SOA Software Policy Manager Console	7.1.0.201406231133	This feature includes a web based user interface for the central Policy Manager governance application. The user interface provides a dashboard and the primary interface for configuration, management and administration of Policy Manager and Service Manager. The console must interact with a Container (may be the same container) configured with the SOA Software Policy Manager Services to fulfill the core central governance application requirements.	
SOA Software Policy Manager Services	7.1.0.201403191452	This feature includes services provided by the central Policy Manager governance application. These services include, but are not limited to, UDDIv2 and UDDIv3, WS-MetadataExchange, SOA Container Configuration, an XACML Policy Decision Point, a WS-Trust Security Token Service, Alert reporting, and RESTful interfaces to the governance model. In addition, this feature includes engines for performing Quality of Service calculations and health and status monitoring.	
SOA Software Scheduled Jobs	7.1.0.201403191452	This feature includes Scheduled Jobs required by PM Engine.	
SOA Software Security Services	7.1.0.201403191452	This feature includes Security Services required by PM Engine.	
SOA Software Tomcat Agent	7.1.0.201403191452	This feature is the policy enforcement point for the Apache Tomcat application server and provides WS-Policy enforcement for web services deployed to Tomcat. It can only be deployed in a Container deployed in a Tomcat instance and only supports the Apache Axis 1.4 SOAP framework.	

### 2.1 Install Internet-facing and administration applications on separate containers

There are two components to this:

- 1) The Community Manager should not be installed on the same container as Policy Manager Console
- 2) The Community Manager User Interface and APIs provide both consumer-facing and administrative functions. If needed by your security constraints, the administrative functions can be disabled in Community Manager. This will allow you to install different instances of Community Manager on different containers – and disable the administration functionality in the Internet-facing instance. To disable the administrative functionality in the Community Manager:

In the admin console, configure the following:

```
com.soa.atmosphere ->
    atmosphere.config.denyUserRoles=SiteAdmin,BusinessAdmin,ApiAdmin
```

## 2.2 Configure all listeners, internal and external as HTTPS only

This is accomplished in two places in the product. Firstly, when the container starts up, it supports an Admin application (/admin). The port and associated transport settings are configurable in the /instances/[container\_name]/system.properties file for each container.

Scope: All Containers

```
#Config for pm
#Thu Jul 10 23:47:51 PDT 2014
product.home=file\:/Users/example/soa/sm70/
org.eclipse.jetty.server.Request.maxFormContentSize=500000
felix.cm.dir=${felix.cache.rootdir}/cm
org.osgi.service.http.port.secure=9900
com.soa.provision.file.dir=${felix.cache.rootdir}/deploy
product.home.dir=/Users/alistairfarquharson/soa/b962/sm70
com.soa.snapshot.directory=${felix.cache.rootdir}/snapshot
com.soa.provision.noInitialDelay=true
com.soa.http.host.secure=127.0.0.1
com.soa.http.bind.all.secure=true
com.soa.provision.bundles.start=true
com.soa.provision.poll=2000
org.eclipse.jetty.servlet.SessionCookie=JSESSIONID_pm
felix.shutdown.hook=false
container.name=[container_name]
```

Note above the \*.secure syntax used for the 3 settings.

Secondly, the listeners for the applications in the container are configured from within Policy Manager at Containers->[container\_name]->Details->Inbound Listeners. Options for configuring port and PKI are available.

## 2.3 Configure the Admin console (/admin) on a separate port

As shown above, this is configurable in the /instances/[container\_name]/system.properties file for each container. The Admin console and the applications running in the console should ideally not be configured on the same port. This will allow you to isolate the Admin console from the Internet.

Scope: All Containers

```
#Config for pm
#Thu Jul 10 23:47:51 PDT 2014
product.home=file\:/Users/example/soa/sm70/
org.eclipse.jetty.server.Request.maxFormContentSize=500000
felix.cm.dir=${felix.cache.rootdir}/cm
org.osgi.service.http.port.secure=9900
com.soa.provision.file.dir=${felix.cache.rootdir}/deploy
product.home.dir=/Users/alistairfarquharson/soa/b962/sm70
com.soa.snapshot.directory=${felix.cache.rootdir}/snapshot
com.soa.provision.noInitialDelay=true
```

```
com.soa.http.host.secure=127.0.0.1
com.soa.http.bind.all.secure=true
com.soa.provision.bundles.start=true
com.soa.provision.poll=2000
org.eclipse.jetty.servlet.SessionCookie=JSESSIONID_pm
felix.shutdown.hook=false
container.name=[container_name]
```

### 3 Configuration Settings

This section covers settings and tuning parameters in the product related to hardening.

#### 3.1 Add the unlimited strength policy to the JDK

To support long passwords when importing PKI from Java Keystores, you will need to install the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. This is dependent on the JDK version being used and is available from Oracle. To install, copy the `US_export_policy.jar` and `local_policy.jar` files to the `/lib/security` directory for the JDK.

Scope: All Containers

#### 3.2 Configure the product to ignore downstream cookies

This prevents the product from automatically storing and forwarding any cookies retrieved from the downstream APIs and Services.

Scope: All Containers

In the admin console, configure the following:

```
com.soa.http.client.core ->
    http.client.params.cookiePolicy=ignoreCookies
```

#### 3.3 Configure secure cookies

This sets the product to only use secure cookies.

Scope: All Containers

In the admin console, configure the following:

```
com.soa.transport.jetty ->
    session.manager.factory.secureCookies=true
```

#### 3.4 Ignore downstream cookies

This sets the product to ignore any downstream cookies.

Scope: All Containers

```
com.soa.http.client.core ->
    http.client.params.cookiePolicy=ignoreCookies
```

#### 3.5 Disabling SSLv3

This configured the product to disable SSLv3.

Scope: All Containers

```
com.soa.transport.jetty ->
    http.incoming.transport.config.enabledProtocols=SSLv2HELLO,TLSv1,TLSv1.1,
    TLSv1.2
```

### 3.6 Restrict the cipher suites used

Use only stronger cipher suites for SSL

Scope: All Containers

In the admin console, configure the following:

```
com.soa.transport.jetty ->
    http.incoming.transport.config.cipherSuites=SSL_RSA_WITH_RC4_128_MD5
    ,SSL_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_W
    ITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3
    DES_EDE_CBC_SHA
```

### 3.7 Prevent Forward Proxying

Prevent unauthenticated users from initiating arbitrary internal connections from the Community Manager portal.

Scope: Community Manager Containers

```
com.soa.atmosphere.forwardproxy ->
    forward.proxy.allowedHosts=<Network Director Host(s) and/or Load
    Balancer host>
```

Values are comma separated.

### 3.8 Header Propagation in Network Director

Prevent the automatic propagation of certain HTTP headers through the Network Director and also configure a translation of the X-Forwarded-Host header.

Scope: Network Director Containers

In the admin console, configure the following:

```
com.soa.http.client.core ->
    block.headers.interceptor.blocked=content-type,content-
    length,content-range,content-md5,host,expect,keep-
    alive,connection,transfer-encoding,atmo-forward-to,atmo-forwarded-
    from

    header.formatter.interceptor.templates=replace=X-Forwarded-
    Host:{host}
```



### 3.9 Header Propagation in Community Manager Subsystem

Prevent the automatic propagation of certain HTTP headers through the Network Director and also configure a NULL (none) translation of the X-Forwarded-Host header.

Scope: Community Manager Containers

In the admin console, configure the following:

```
com.soa.http.client.core ->
    block.headers.interceptor.blocked=content-type,content-
    length,content-range,content-md5,host,expect,keep-
    alive,connection,transfer-encoding

    header.formatter.interceptor.templates=
```

### 3.10 Tune the API Security Credential Cache

You can configure the expiration period and refresh time for the security cache for API calls.

Scope: Network Director Containers

In the admin console, optionally configure the following:

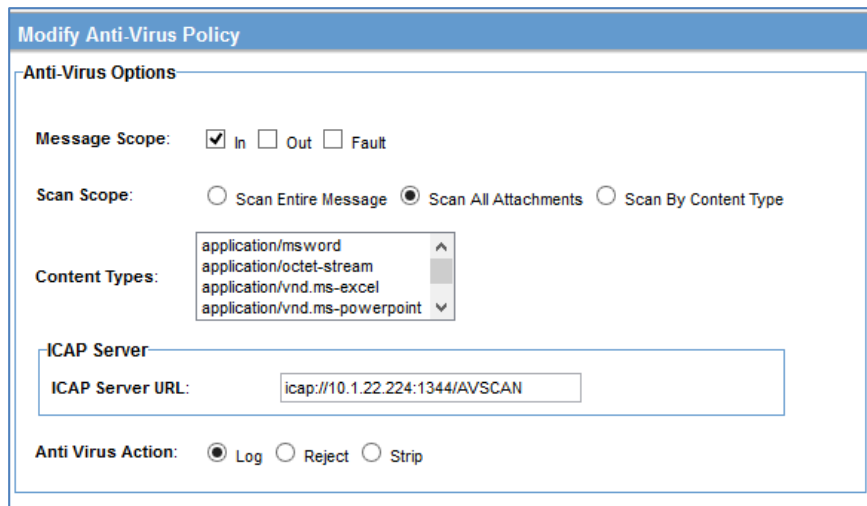
```
com.soa.api.security ->
    com.soa.api.security.cache.expirationPeriod=3600000
    com.soa.api.security.cache.refreshTime=300000
```

### 3.11 Configure the Anti-virus Policy to scan for uploaded files

The Anti-virus policy scans for files that are uploaded from the Community Manager Portal.

Scope: All Community Manager Containers

In the Policy Manager Console, create an Anti-Virus Operational Policy and configure the policy.



**Modify Anti-Virus Policy**

**Anti-Virus Options**

**Message Scope:** ☒ In ☐ Out ☐ Fault

**Scan Scope:** ☐ Scan Entire Message ☒ Scan All Attachments ☐ Scan By Content Type

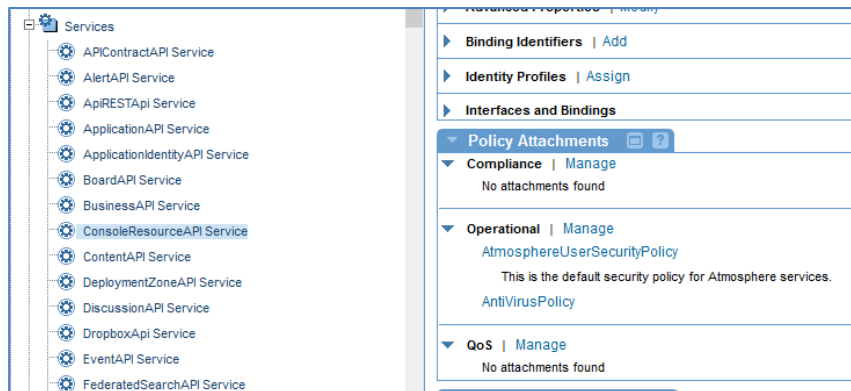
**Content Types:** application/msword, application/octet-stream, application/vnd.ms-excel, application/vnd.ms-powerpoint

**ICAP Server**

**ICAP Server URL:** icap://10.1.22.224:1344/AVSCAN

**Anti Virus Action:** ☒ Log ☐ Reject ☐ Strip

Attach this policy to the ConsoleResourceAPIService and the ContentAPIService in the Policy Manager -> Community Manager node in the Policy Manager Console Organization tree.



### 3.12 Enabling CSRF protection


You can enable and disable CSRF protection in the Policy Manager and Community Manager User Interfaces.

**Scope:** All Community Manager and Policy Manager Containers

Due to the fact that Policy Manager is not Internet-facing, it is disabled by default. You can enable the CSRF protection in the Policy Manager in the admin console:

```
com.soa.console.csrf ->
    org.owasp.csrfguard.Enabled=true
```

In Community Manager, CSRF configuration can be found under Administration -> Config -> Security Settings:

 **Business Security Settings**

The settings below allow you to control the level of security associated with platform elements, and to control certain elements relating to security that affect platform users.

**CSRF Support for Read Requests:**  
☐ Enabled  
☒ Disabled

**CSRF Support for Write Requests:**  
☒ Enabled  
☐ Disabled

**Allow User Enum:**  
☒ Enabled  
☐ Disabled

**Encrypt Challenge Answers:**  
☒ Enabled  
☐ Disabled

**Challenge Count:**

**Allow User to Modify Profile:**  
☐ Enabled  
☒ Disabled

### 3.13 Adding XSS exclusions

Cross-site-scripting (XSS) is a way to inject client-side script into Web pages viewed by other users.

Scope: All Community Manager and Policy Manager Containers

To configure any exceptions to the exclusion policy:

```
com.soa.console.xss ->
    exceptionURLs=[COMMA DELIMITED LIST]
```

To configure any new keywords that should be excluded:

```
com.soa.console.xss ->
    keywords=[COMMA DELIMITED LIST]
```

To turn XSS validation on/off:

```
com.soa.console.xss ->
    validate=[true|false]
```

### 3.14 Turning off User Account Enumeration

User Account Enumeration occurs when the Community Manager user interface provides direct feedback to a user during the signup and registration processes to the effect that a user account already exists or is already registered. If this is turned off, no useful feedback is provided to the user, minimizing the security risk, but decreasing usability.

Scope: All Community Manager Containers

In Community Manager, User Account Enumeration configuration can be found under Administration -> Config -> Security Settings:

**Business Security Settings**

The settings below allow you to control the level of security associated with platform elements, and to control certain elements relating to security that affect platform users.

**CSRF Support for Read Requests:**  
☐ Enabled  
☒ Disabled

**CSRF Support for Write Requests:**  
☒ Enabled  
☐ Disabled

**Allow User Enum:**  
☒ Enabled  
☐ Disabled

**Encrypt Challenge Answers:**  
☒ Enabled  
☐ Disabled

**Challenge Count:**

**Allow User to Modify Profile:**  
☐ Enabled  
☒ Disabled

### 3.15 Configuring Challenge Questions/Answers

Challenge Questions/Answers are often required to increase security around password reset. When signing up to the platform, the user must provide the answer to one or more security questions, if the platform is set up to require them. The user's answers are stored in the database, and the user must answer one or more security questions on demand to perform certain functions such as resetting a password or changing the user profile.

Scope: All Community Manager Containers

In Community Manager, the Challenge Questions/Answers configuration can be found under Administration -> Config -> Users:

Enforce Challenge Questions on Login -> Enabled

Additional settings can be found under Administration -> Config -> Security Settings:

**Business Security Settings**

The settings below allow you to control the level of security associated with platform elements, and to control certain elements relating to security that affect platform users.

**CSRF Support for Read Requests:**  
☐ Enabled  
☒ Disabled

**CSRF Support for Write Requests:**  
☒ Enabled  
☐ Disabled

**Allow User Enum:**  
☒ Enabled  
☐ Disabled

**Encrypt Challenge Answers:**  
☒ Enabled  
☐ Disabled

**Challenge Count:**

**Allow User to Modify Profile:**  
☐ Enabled  
☒ Disabled

Configuration of the actual questions available can be done via an API call into the system. For details of the API call see:

[http://docs.soa.com/cm/api/businesses/m\\_businesses\\_saveChallenges.htm](http://docs.soa.com/cm/api/businesses/m_businesses_saveChallenges.htm)

### 3.16 Disallowing User Profile Modification

User Profile Modification permits a user access to their own profile for modification. In some circumstances, you may wish to prevent this (e.g. when user accounts are pre-provisioned).

Scope: All Community Manager Containers

In Community Manager, User Profile Modification configuration can be found under Administration -> Config -> Security Settings:

### 3.17 Configuring Account Login Rules

The account login rules may include many options regarding failure attempts allowed, account suspension times, auto-login, etc.

Scope: Community Manager

These login policies may be set via an API call into the system or a direct DB query. For details of the API call see:

[http://docs.soa.com/cm/api/businesses/m\\_businesses\\_updateLoginPolicy.htm](http://docs.soa.com/cm/api/businesses/m_businesses_updateLoginPolicy.htm)

If using a DB query, the syntax will be something like:

```
-- Login Rules
update LOGIN_RULES set MAXATTEMPTS=3, ATTEMPTSPERIOD=1, SUSPENSIONTIME=30,
AUTO_LOGIN_EXT_DOMAIN='com.soa.feature.enabled' where TENANTID = (select
TENANTID from TENANTS where FEDMEMBERID='[YOUR TENANT ID]');
```

### 3.18 Configuring Password Complexity Rules

Password requirements (rules) may include many options regarding length, special characters, etc.

Scope: Community Manager

These password rules may be set via an API call into the system or a direct DB query. For details of the API call see:

[http://docs.akana.com/cm/api/businesses/m\\_businesses\\_updatePasswordPolicy.htm](http://docs.akana.com/cm/api/businesses/m_businesses_updatePasswordPolicy.htm)

If using a DB query, the syntax will be something like:

```
-- Password Rules
update PASSWORD_RULES set MINLENGTH=8, MAXLENGTH=20, MINLETTERS=1,
MINNUMBERS=1, ALLOWEDSPECCHARS='%&_?#=-', CANCONTAINSPACES='N',
ISCASESENSITIVE='N' where TENANTID = (select TENANTID from TENANTS where
FEDMEMBERID='[YOUR TENANT ID]');
```

### 3.19 Configuring X-FRAME-OPTIONS Header

The X-FRAME-OPTIONS header plays a role in determining if and how the user interface can be embedded within an iFrame in a 3<sup>rd</sup> party site.

Scope: All Community Manager and Policy Manager Containers

To configure Community Manager:

```
com.soa.atmosphere.console ->
    atmosphere.console.config.xFrameOptions=[DESIRED HEADER]
```

To configure Policy Manager:

```
com.soa.console.xss ->
    xFrameOptions=[DESIRED HEADER]
```

## 4 About Akana

Akana is a leading provider of unified governance automation products that enable organizations to successfully plan, build, and run enterprise services. The world's largest companies including Bank of America, Verizon, and Pfizer use Akana solutions to transform their business. For more information, please visit <http://www.soa.com>.

Akana, Policy Manager, Portfolio Manager, Repository Manager, Service Manager, and SOLA are trademarks of Akana, Inc. All other product and company names herein may be trademarks and/or registered trademarks of their registered owners.

Akana, Inc.

12100 Wilshire Blvd, Suite 1800

Los Angeles, CA 90025

310-826-1317

[www.akana.com](http://www.akana.com)

[info@soa.com](mailto:info@soa.com)

Copyright © 2015 by Akana, Inc.

Disclaimer: The information provided in this document is provided "AS IS" WITHOUT ANY WARRANTIES OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY. Akana may make changes to this document at any time without notice. All comparisons, functionalities and measures as related to similar products and services offered by other vendors are based on Akana's internal assessment and/or publicly available information of Akana and other vendor product features, unless otherwise specifically stated. Reliance by you on these assessments / comparative assessments are to be made solely on your own discretion and at your own risk. The content of this document may be out of date, and Akana makes no commitment to update this content. This document may refer to products, programs or services that are not available in your country. Consult your local SOA Software business contact for information regarding the products, programs and services that may be available to you. Applicable law may not allow the exclusion of implied warranties, so the above exclusion may not apply to you.