SecureLogix®
We see your voice®

PolicyGuru®

Meta-Policy Controller v3.1.2

Standalone CAS Agent Installation and Configuration Guide

About SecureLogix

For more than 20 years, SecureLogix has profiled, tracked and defended customers against the schemes and threats plaguing unified communications networks. We've developed patented technology and assembled the most skilled team in the industry to monitor and protect some of the world's largest and most complex contact centers and voice networks.

We're not the largest IT vendor; we're the one with the start-up agility and decades of unrivaled enterprise experience. The one that is there when you need us, with superhero level support.

For more information about SecureLogix and its products and services, visit us on the Web at *https://securelogix.com/*.

Corporate Headquarters:
SecureLogix Corporation
13750 San Pedro, Suite 820
San Antonio, Texas 78232
Telephone: 210-402-9669 (non-sales)
Fax: 210-402-6996
Email: *info@securelogix.com*
Website: *https://www.securelogix.com*

Sales:
Telephone: 1-800-817-4837 (North America)
Email: *sales@securelogix.com*

Customer Support:
Telephone: 1-877-SLC-4HELP
Email: *support@securelogix.com*
Web Page: *https://support.securelogix.com*

Training:
Email: *elearning@securelogix.com*

Documentation:
Email: *docs@securelogix.com*
Knowledge Base: *https://support.securelogix.com*

IMPORTANT NOTICE:

The content of this manual is subject to change without notice. SecureLogix assumes no responsibility or liability for any errors or inaccuracies that may be contained herein or to correct the same.

ETM, We See Your Voice, SecureLogix, and the SecureLogix Emblem are registered trademarks and registered service marks of SecureLogix Corporation in the U.S.A. and other countries. PolicyGuru is a registered trademark of SecureLogix Corporation in the U.S.A. Orchestra One, Call Secure, and Call Defense are trademarks and service marks of SecureLogix Corporation in the U.S.A. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

This product is protected by one or more of the following patents:
US 11,349,987 B2 and US 11,356,551 B2. U.S. Patent Pending.

PolicyGuru is used herein as shorthand notation to refer to the PolicyGuru® Solution.

Orchestra One is used herein as shorthand notation to refer to the Orchestra One™ Call Authentication Service.

This product also includes code written by other third parties.

Additional details regarding other third party code included in this product, including applicable copyright, legal, and licensing notices, are available in the "licenses" directories included with the third-party code.

Customer Support
for Your SecureLogix® Solution

1-877-SLC-4HELP

(1-877-752-4435)

support@securelogix.com

https://support.securelogix.com

**SecureLogix Corporation offers telephone,
email, and web-based support.
For details on warranty information
and support contracts, see our web site at**

https://support.securelogix.com

Contents

PolicyGuru® Solution v3.1.2 Standalone CAS Agent Installation and Configuration

Introduction

The PolicyGuru® Solution v3.1.2 Standalone CAS Agent is a version of the PolicyGuru® Solution v3.1.2 CAS Agent that can be deployed on its own system, separate from the Mediation Server, to reduce resource load on the Mediation Server for large Orchestra One™ Call Authentication System (CAS) deployments. This feature also enables/facilitates High Availability (HA) for the CAS Agent service, planned for a future release—separating this component enables adding functionality like redundancy and failover.

The Standalone CAS Agent is verified to work with both the PolicyGuru v3.1.2 Mediation Server and the PolicyGuru v2.6.x Mediation Server.

The Standalone CAS Agent is deployed as an update to an existing PolicyGuru System. You must have v2.6.x or v3.1.2 installed to implement this feature.

Installation

The Standalone CAS Agent system can be deployed onto a Virtual Machine using the Standalone CAS Agent OVA image (which includes appropriate system resources and pre-installed Standalone CAS Agent Software), or it can be installed onto an existing system using the Standalone CAS Agent YUM repo. For either installation method, the system is expected to be co-located on the same Local Area Network (LAN) with the Mediation Server.

YUM Repo Installation

For installation on an existing system using the YUM repo, start with a CentOS 7 system with a minimum of 4 cores, 8 GB RAM, 150 GB storage, and Gigabit networking. Prepare that system for installation using the PG Houston (3.0.2) CentOS and Software Installation Guide.

To install the Standalone CAS Agent software

1. Make the **kendall23.casagent** YUM repo available for YUM installation.
2. If Amazon Corretto 8 Java is not already installed on the system, install the latest available RPM (currently **java-1.8.0-amazon-corretto-devel-1.8.0_352.b08-1.x86_64.rpm**).
3. Install the Standalone CAS Agent packages using the command :

```
yum groupinstall cas_agent
```

4. If not already enabled in **systemd**, enable the **iptables** and **ngp-CasAgentServer.service** services using the following commands:

   ```
   systemctl enable iptables
   ```

   ```
   systemctl enable ngp-CasAgentServer.service
   ```

   This enablement will cause those services to be started when the system starts up.

5. When interfacing with a PolicyGuru v2.6.x Mediation Server, copy the **jboss-client.jar** file from the **/opt/ngp/jboss-as-7.2.0.Final/bin/client/** folder on the PolicyGuru v2.6.x Mediation Server into the **/opt/ngp/pg-cas-agent/lib** folder on the Standalone CAS Agent system.

******* Continue with “Configuration” on page 7. ********

OVA Installation

To install using the OVA

- Install the OVA as usual, and then continue with “Configuration” below.

Configuration

Standalone CAS Agent configuration generally follows the configuration detailed in PG 3.1.2 CAS Agent Configuration Guide (current as of kendall21) and its child pages PG 3.1.2 CAS Agent Correlation Mode Configuration (current as of kendall21) , PG 3.1.2 CAS Agent AuthOnly Mode Configuration (current as of kendall21) , and PG 3.1.2 CAS Agent SIPOnly Mode Configuration (current as of kendall21).

Differences in configuration specific to the Standalone CAS Agent are detailed in “Standalone CAS Agent Configuration Differences” on page 8. Additional required configuration when interfacing with a v2.6 Mediation Server rather than a v3.1.2 Mediation Server is detailed in “Configuration When Interfacing with a v2.6.x Mediation Server” on page 9.

Important: Unless this service is being used on a temporary basis, always configure the Standalone CAS Agent service to automatically start on system startup using the command:

```
systemctl enable ngp-CasAgentServer.service.
```

Use the following procedures to configure the Standalone CAS Agent.

Enabling Standalone CAS Agent Processing

To enable Standalone CAS Agent processing

- On the Standalone CAS Agent server, edit **/opt/ngp/config/pg-cas-agent/agent-config.properties** and set **enabled=true**.
- Set this value to **false** to disable Standalone CAS Agent processing.

WARNING: When using a remote Standalone CAS Agent service, the built-in CAS Agent service on the Mediation Server must be disabled in the **/opt/ngp/config/pg-cas-agent/agent-config.properties** file (**enabled=false**) on the Mediation Server, and the service must be stopped/killed if currently running. Likewise, if the built-in CAS Agent service is being used, a remote Standalone CAS Agent service must be stopped/disabled. Running both the built-in CAS Agent service and a remote Standalone CAS Agent service at the same time will result in conflicts and processing failures.

Selecting and Configuring the Configuration Mode

The three Configuration Modes (Correlation Mode, Auth Only Mode, and SIP Only Mode) detailed in the above referenced guides are available when running the Standalone CAS Agent. However, there are some configuration differences for the Standalone CAS Agent, as described below.

To select the Configuration Mode

- Link **/opt/ngp/config/pg-cas-agent/eipController.json** to the primary configuration file for one of the three modes. The primary configuration files **are /opt/ngp/pg-cas-agent/casAgentCorrelation.json** (Correlation Mode), **/opt/ngp/pg-cas-agent/casAgentAuthOnly.json** (Auth Only Mode), and **/opt/ngp/pg-cas-agent/casAgentSipOnly.json** (SIP Only Mode).

Standalone CAS Agent Configuration Differences

Below are differences from the standard CAS Agent configuration instructions that are specific to the Standalone CAS Agent configuration:

/opt/ngp/pg-cas-agent/correlationAuthXcvr.json

When using **Correlation Mode**, the **brokerURL** in the receiver section of this file should be modified to use the IP address of the Mediation Server rather than **localhost**. Below is an example of that setting:

```
"brokerURL": "tcp://10.1.100.100:61616",
```

/opt/ngp/pg-cas-agent/correlationProbeXcvr.json

When using **Correlation Mode**, the **brokerURL** in the receiver section of this file should be modified to use the IP address of the Mediation Server rather than “**localhost**”. Below is an example of that setting:

```
"brokerURL": "tcp://10.1.100.100:61616",
```

/opt/ngp/pg-cas-agent/casAgentAuthOnly.json

When using **AuthOnly Mode**, the **brokerURL** in the receiver section of this file should be modified to use the IP address of the Mediation Server rather than **localhost**. Below is an example of that setting:

```
"brokerURL": "tcp://10.1.100.100:61616",
```

/opt/ngp/pg-cas-agent/casAgentSipOnly.json

When using **SIPOnly Mode**, the **brokerURL** in the receiver section of this file should be modified to use the IP address of the Mediation Server rather than “**localhost**”. Below is an example of that setting:

```
"brokerURL": "tcp://10.1.100.100:61616",
```

/opt/ngp/pg-cas-agent/authAnswerXcvr.json

When using the **ENUM Response based on CAS Result** feature, the **brokerURL** in the sender section of this file should be modified to use the IP address of the Mediation Server rather than **localhost**. Below is an example of that setting:

```
"brokerURL": "tcp://10.1.100.100:61616",
```

Configuration When Interfacing with a v2.6.x Mediation Server

When interfacing with a PolicyGuru v2.6.x Mediation Server (rather than a v3.1.2 Mediation Server), there are some additional configuration changes and caveats described in the following sections.

jboss-client.jar

As mentioned above in the "Installation" section on page 6, the **jboss-client.jar** file must be obtained from the **/opt/ngp/jboss-as-7.2.0.Final/bin/client/** folder on the PolicyGuru 2.6.x Mediation Server and copied into the **/opt/ngp/pg-cas-agent/lib** folder on the Standalone CAS Agent system.

/opt/ngp/pg-cas-agent/correlationAuthXcvr.json

When using **Correlation Mode**, the receiver section of this file should be modified to be compatible with the HornetQ Message Broker used by the PolicyGuru v2.6.x Mediation Server. In particular, the format/content of the **brokerURL**, **connectionFactory**, and **contextFactory** should be changed, and a new **id** field should be added. (See "Mediation Server id Field Configuration" on page 11 for more information.) For the **brokerURL** field, ensure that the "remote" scheme name and port 4447 are set, in addition to using the IP address of the Mediation Server rather than **localhost**. Below is an example of a modified receiver section:

```
"receiver": {
        "type": "com.securelogix.eip.jms.JMSReceiverThread",
        "name": "Rcvr",
        "threads": "2",
        "flushTimeout": "1000",
        "batchSize": "1",
        "enforceFlushTimeout": "false",
        "consumerName": "pg_cas_agent",
        "connectionFactory": "/jms/RemoteConnectionFactory",
        "destinationType": "queue",
        "brokerURL": "remote://10.1.100.100:4447",
        "id": "msid",
        "contextFactory": "jboss",
        "destination": "detentionCenterNorthboundChannel"
},
```

/opt/ngp/pg-cas-agent/correlationProbeXcvr.json

When using **Correlation Mode**, the receiver section of this file should be modified to be compatible with the HornetQ Message Broker used by the PolicyGuru 2.6.x Mediation Server. In particular, the format/content of the **brokerURL**, **connectionFactory**, and **contextFactory** should be changed, and a new **id** field should be added. (See "Mediation Server id Field Configuration" on page 11 for more information.) For the **brokerURL** field, ensure that the "remote" scheme name and port 4447 are set, in addition to using the IP address of the Mediation Server rather than **localhost**. Below is an example of a modified receiver section:

```
"receiver": {
        "type": "com.securelogix.eip.jms.JMSReceiverThread",
        "name": "Rcvr",
        "threads": "2",
        "flushTimeout": "1000",
        "batchSize": "1",
        "enforceFlushTimeout": "false",
        "consumerName": "pg_cas_agent",
        "connectionFactory": "/jms/RemoteConnectionFactory",
        "destinationType": "queue",
        "brokerURL": "remote://10.1.100.100:4447",
        "id": "msid",
        "contextFactory": "jboss",
        "destination": "probeSipInviteDataChannel"
},
```

/opt/ngp/pg-cas-agent/casAgentAuthOnly.json

When using **AuthOnly Mode**, the receiver section of this file should be modified to be compatible with the HornetQ Message Broker used by the PolicyGuru 2.6.x Mediation Server. In particular, the format/content of the **brokerURL**, **connectionFactory**, and **contextFactory** should be changed, and a new **id** field should be added. (See “Mediation Server id Field Configuration” on page 11 for more information.). For the **brokerURL** field, ensure that the “remote” scheme name and port 4447 are set, in addition to using the IP address of the Mediation Server rather than **localhost**. Below is an example of a modified receiver section:

```
 "receiver": {
         "type": "com.securelogix.eip.jms.JMSReceiverThread",
         "name": "Rcvr",
         "threads": "2",
         "flushTimeout": "1000",
         "batchSize": "1",
         "enforceFlushTimeout": "false",
         "consumerName": "pg_cas_agent",
         "connectionFactory": "/jms/RemoteConnectionFactory",
         "destinationType": "queue",
         "brokerURL": "remote://10.1.100.100:4447",
         "id": "msid",
         "contextFactory": "jboss",
         "destination": "detentionCenterNorthboundChannel"
 },
```

/opt/ngp/pg-cas-agent/casAgentSipOnly.json

When using **SIPOnly Mode**, the receiver section of this file should be modified to be compatible with the HornetQ Message Broker used by the PolicyGuru 2.6.x Mediation Server. In particular, the format/content of the **brokerURL**, **connectionFactory**, and **contextFactory** should be changed, and a new **id** field should be added. (See “Mediation Server id Field Configuration” on page 11 for more information.). For the **brokerURL** field, ensure that the “remote” scheme name and port 4447 are set, in addition to using the IP address of the Mediation Server rather than **localhost**. Below is an example of a modified receiver section:

```
"receiver": {
        "type": "com.securelogix.eip.jms.JMSReceiverThread",
        "name": "Rcvr",
        "threads": "2",
        "flushTimeout": "1000",
        "batchSize": "1",
        "enforceFlushTimeout": "false",
        "consumerName": "pg_cas_agent",
        "connectionFactory": "/jms/RemoteConnectionFactory",
        "destinationType": "queue",
        "brokerURL": "remote://10.1.100.100:4447",
        "id": "msid",
        "contextFactory": "jboss",
        "destination": "probeSipInviteDataChannel"
},
```

Mediation Server id Field Configuration

As noted in the sections above, an **id** field has been added for JMS connections to HornetQ on the PolicyGuru v2.6.x Mediation Server. This **id** field is a reference to a username/password pair that is stored in the SLC Password Vault on the Standalone CAS Agent system.

On the Standalone CAS Agent system, add a JMS username/password pair to the SLC Password Vault using a command such as “/opt/ngp/util/security/slc-pwvault store msid esbrest SecureLogix1!” where “msid” is the **id** field value added to the above configuration files and “esbrest SecureLogix1!” is the username and password of a JMS user on the PolicyGuru 2.6.x Mediation Server. The esbrest/SecureLogix1! username/password pair is a valid pair to use.

/opt/ngp/pg-cas-agent/authAnswerXcvr.json

Although the Standalone CAS Agent supports the “ENUM Response Based on CAS Result” feature, the PolicyGuru v2.6.x System does **not** support this feature. Therefore, this feature should **not** be configured/used when interfacing with a v2.6.x Mediation Server.

Service Control and Status

Configure the Standalone CAS Agent service to automatically start on system startup (enable) or not automatically start on system startup (disable) using the following commands. For all normal production systems, the service should be enabled.

- **systemctl enable ngp-CasAgentServer.service**
- **systemctl disable ngp-CasAgentServer.service**

To stop, start, or restart the Standalone CAS Agent service, use the following commands:

- **systemctl stop ngp-CasAgentServer.service**
- **systemctl start ngp-CasAgentServer.service**
- **systemctl restart ngp-CasAgentServer.service**

The status of the Standalone CAS Agent service can be obtained through the following commands:

- **systemctl status ngp-CasAgentServer.service**
- **systemctl list-units 'ngp-*' -a**

Logging

Application logs are written to the **/opt/ngp/pg-cas-agent/cas_agent.log** and previous logs are rolled over to the /**opt/ngp/pg-cas-agent/logs** folder.

To modify the log level of the **cas_agent.log** and/or modify the rollover/deletion policy of the **cas_agent.log**, modify the **/opt/ngp/pg-cas-agent/log4j2.xml** file (which is linked to **/opt/ngp/log/pg-cas-agent/log4j2.xml**).

Available log levels are **fatal**, **error**, **warn**, **info** (the default), **debug**, and **trace** (most verbose).