

Alarm Monitoring Standard Edition (AM-SE)

Technical Considerations

**April 14, 2015**

Created by: Genesys Customer Care

Notice

Copyright © 2015 Genesys Telecommunications Laboratories, Inc. All rights reserved.

Genesys Telecommunications Laboratories, Inc.

2001 Junipero Serra Blvd,

Daly City, CA 94014

Phone: 1-888-GENESYS

Fax: 1-650-466-1260

The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

About Genesys

Genesys Telecommunications Laboratories, Inc., a subsidiary of Alcatel-Lucent, pioneered the field of Computer-Telephony Integration (CTI) and today is the leading provider of infrastructure independent contact center solutions for the enterprise, service provider, and e-business markets. With its ability to integrate interactions across all media types, including the Web and traditional voice, Genesys software helps businesses provide a consistent customer interaction experience.

Trademarks

Genesys and the Genesys logo are registered trademarks of Genesys Telecommunications Laboratories, Inc. UNIX is a registered trademark of The Open Group in the United States and other countries. Microsoft, Windows, Windows 2000, Windows NT, Windows 2003, Windows XP, and Windows Vista are registered trademarks of Microsoft Corporation. All other trademarks and trade names referred to in this document are the property of other companies.

Table of Contents

[1. **Introduction** 4](#_Toc416376742)

[2. **Service Architecture** 5](#_Toc416376743)

[3. **The Appliance** 5](#_Toc416376744)

[4. **Firewall Requirements** 5](#_Toc416376745)

[5. **Other requirements** 6](#_Toc416376746)

[6. **Server Requirements** 6](#_Toc416376747)

[7. **Communication** 7](#_Toc416376748)

[8. **Remote Access** 7](#_Toc416376749)

[9. **Appliance Provisioning** 8](#_Toc416376750)

# **Introductio**

Genesys customers have come to rely heavily on the functionality they gain from the Genesys Contact Centre platform. As such, the highest level of availability is required for these deployments in order to meet the business needs. Genesys has developed a set of best practices based on industry standards in order to help proactively prevent and more quickly resolve issues within the platform.

The Genesys Alarm Monitoring Standard Edition (AM-SE) includes an appliance residing on the customer premise, which allows the Genesys team better insight into proactively discovering and responding to incidents.

The appliance resides on the customer premise and creates an encrypted connection to the central hub. The appliance initiates all communication between the central hub and the appliance (internal, outbound) thus drastically reducing any security risk of unauthorized inbound customer traffic. When the appliance receives an alarm, it forwards the alarm to the central hub database for presentation via the monitoring portal.

This document describes many of the typical implementation scenarios and risk mitigation strategies that can be performed to ensure that the computing environment at the customer site remains secure while enhancing the availability of their contact center environment. It should also be noted that Genesys is willing to work with the customer’s security group to ensure that the monitoring platform meets or exceeds the security standards in place at the customer’s site and will tailor the delivery of this service as necessary to align with those standards.

The security topics discussed in this document are:

Access - who has the permissions and what they can do.

Authentication - is the client who he/she/it claims to be?

Connection – a secure, bi-directional connection between two appliance hubs (management servers)

# **Service Architecture**

The following diagram depicts the overall service architecture. The Customer Alarm Monitoring (CAM) communicates with the central hub via a secure encrypted connection. Connections from the appliance to the central hub are outbound connections only. This connection enables secure online communications between appliances and the central hub. All data exchanged using this connection is encrypted and authenticated and send to Genesys CC Central Hub/Collector via a SSL tunnel..



Access from the appliance to the Hub is as follows

|  |  |
| --- | --- |
| CAM → Central Hub | **IP: 208.79.170.12 (alarm.genesys.com) (Port 443)** |

The CAM is deployed in the customer premises.

The CAM is the main customer component of the AM-SE enabling end-users to supply the support organization with current and historical alarm data. The support representatives can then use this information stored and viewable via the Portal on the Central Hub to diagnose, troubleshoot, and resolve incidents.

The CAM is installed at a customer site, where it communicates with the Solution Control Server (SCS). The CAM listens for SCS alarms and forward those that belong to the standard alarm list to the Customer Alarm Collector (CAC).

Upon start of the CAM software, it creates an encrypted secure connection to the CAC. It then connects to the Configuration Server and determine the SCS host and port. It then subscribes to receive all the alarms for the standard list of alarm conditions. The CAM gets notified any time a new alarm is created in SCS. CAM check if the alarm belongs to the standard list of alarm conditions and sends the alarm to CAC using the encrypted secure connection for further processing.

Upon receipt of new alarms from the CAM, CAC adds it the Database. It will optionally send the alarm to the Network Monitoring System (NMS) so that the alarm can be visualized and also creates a popup on the Mobile Device, if configured and subscribed to receive such notifications.

# **Firewall Requirements**

**Appliance Communications**

* **443**/TCP: (Outbound only) for the TCP/IP connection back to Central Hub

 **Central Hub IP address 208.79.170.12 (Port 443)**

**Monitoring Portal**

* Users that will be accessing the Monitoring Portal web interface will require port 443 access to proactive.genesyslab.com.

**Remote Access**

* Port 443 to ts-bomgar-ca.genesyslab.com -198.164.227.30 **to allow Bomgar Remote Access**

# **Other requirements**

* Java 1.8

**Risk mitigation for appliance**

* The appliance can be isolated by a Firewall where only permitted protocols can be permitted and logged from the Monitoring Platform to the SCS and Configuration Server.

# **Server Requirements**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Deployment size** | **Physical or virtual server requirements** |
| **Processor (XEON-class 2.0 GHz or better)** | **Memory** |
| Modest deployment | Dual quad-core processor | 4 GB to 8 GB |

# **Communication**

The appliance and the Central Hub exchange information through an encrypted secure TCP/IP connection that ensures both authentication and encryption of the data.

Each appliance transmits information to the Central Hub and retrieves information via connection to the SCS.

This method can be used even when firewalls exist, because customers are allowing **443** outbound and the appliance always initiates communication with the Central Hub.

## Encryption

The appliance connection to the central hub is SSL / TLS V1.1 and TLC V1.2. The supported ciphers are RSA Key Exchange, AES-128-CBC cipher and SHA hash function.

# **CAM Provisioning**

 is responsible for providing hardware (or a virtual machine) for the appliance (s). We understand that customer owned hardware (or VM) must be built based on the customer’s specific server specifications. This is definitely something that Genesys can work with the customer to define. The software needed is detailed in the appliance section.

A separate installation guide provides detailed instructions on how to install the CAM. At a high level, the CAM installation package can be downloaded from the Genesys Care web site. Once all the pre-requisite information is available (e.g. Configuration Server access details, license etc.), the CAM can be installed.