Genesys Monitoring Appliance
Technical Considerations

June 20, 2017

Created by: Genesys Customer Care

NOTICE

Genesys Telecommunications Laboratories, Inc.
2001 Junipero Serra Blvd,
Daly City, CA 94014

Phone: 1-888-GENESYS
Fax: 1-650-466-1260

ABOUT GENESYS

Genesys Telecommunications Laboratories, Inc., 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

Table of Contents

1. Introduction

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 Monitoring Platform 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 SSL tunnel to the central hub. All communication between the central hub and the appliance is initiated by the appliance (internal, outbound) thus drastically reducing any security risk of unauthorized inbound customer traffic. When the appliance receives an alarm, it is forwarded 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.

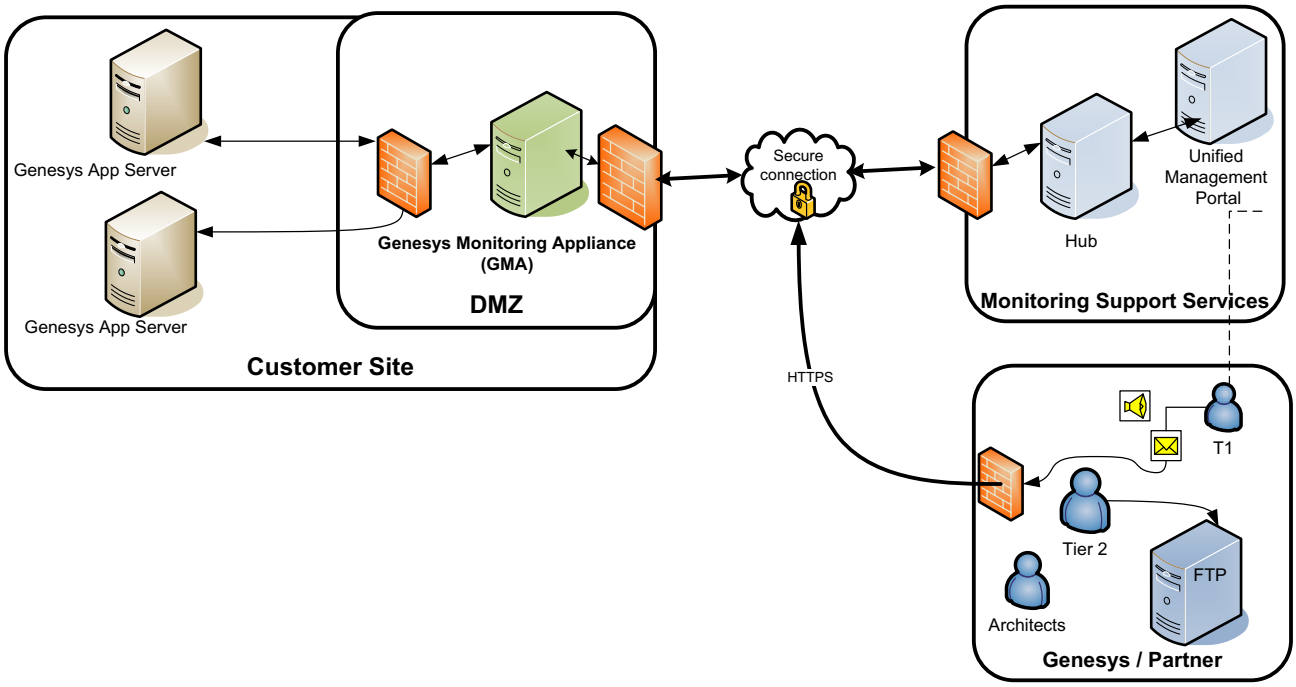
Authentication - is the client who he/she/it claims to be?

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

2. Service Architecture

The following diagram depicts the overall service architecture. The appliance communicates with the central hub via a SSL tunnel. Connections from the appliance to the central hub are outbound connections only. The SSL tunnel enables secure online communications between appliances and the

central hub. All data exchanged using the SSL tunnel is sent using secured proprietary protocol, which means that data is encrypted and authenticated.



Access from the appliance to the Hub is as follows

Appliance → Concentrator Hub	IP **52.42.14.194 (Port 48003)**

Probes are small dedicated pieces of software that monitor specific resources or events. Each Probe can be easily configured for your own specific monitoring requirements. In agent-less deployments, probes are not installed and the data is collected via scripts executed from the Relay Hub.

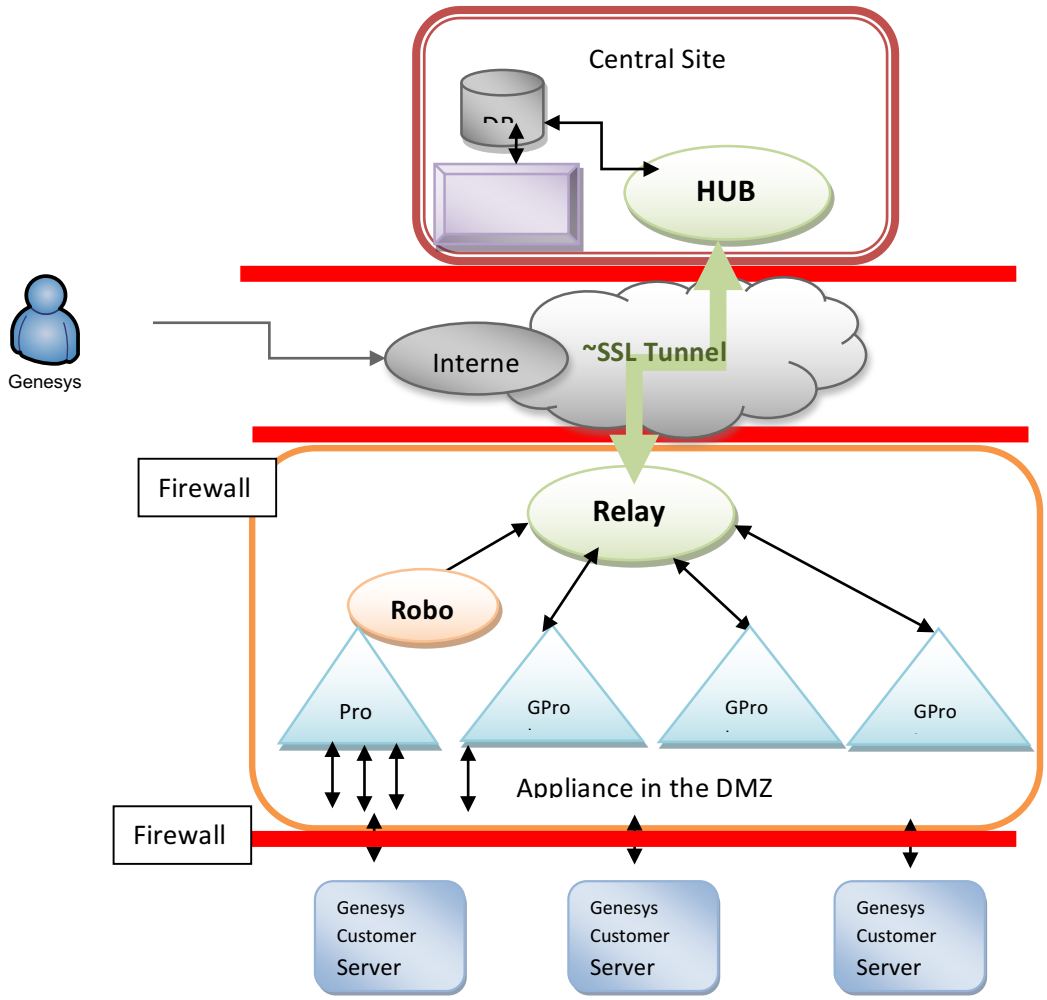
The **Robot** is the first line of management for the Probes. The Robot starts and stops the Probes at the required times, collects, queues and forwards messages from the Probes onto the specified Relay HUB. For agent-less deployment, scripts will collect the information. For agent-based deployments, each computer that is being monitored by a Probe will need a Robot (i.e. agent) installed on it.

The **appliance runs the Relay hub probe that acts as** a message concentrator and re-distributor. It is the collection point for all messages coming from the various installed Robots. Many other components can connect to the appliance to receive dedicated messages and perform other specific activities

The appliance is deployed in the customer premises.

- The appliance should be viewed as a message-bus serving client and server processes connected to it by providing a set of services. The two major components of the Appliance are the Robot and Hub processes. They provide the client/server applications with an entry-point (Robot) and an exit-point (Hub) to/from the Appliance. The messages flow on the bus using routing and naming schemes.
- The illustration below shows the relationships between the various key components of the monitoring platform. Whenever a message is generated by a probe (by issuing a publishing request), the message is picked up by the Robot spooler and passed on to the Robot's primary Hub. The Hub dispatches the message to clients subscribing to the subject which the message is posted under.

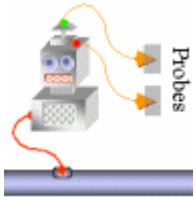
The solution consists of the appliance (Hub-Relays), robots and probes. A typical installation may look like this:



GProbe : Genesys Probe which runs the scripts for agent-less solution

For the purposes of this document, the term node may mean a **Hub**, **robot** or **probe**. Client is a GUI or a probe that can execute a command on other nodes. A complete solution with GUI's and probes that logically belong together is called an application. A **domain** is a collection of one or more Hubs with robots and probes that are logically grouped together. A **robot** consists of a **controller** and a **spooler**

A Robot (Agent) with the active probe publishes messages (the yellow indicator) onto the Message-bus. The message is received by the Robot spooler, which sends (**unless configured to spool to disk)** the message to the Hub that manages this Robot. Note that messages will be bulked together in order to increase the message flow from the Robot to the Appliance. The client will perceive that the message it passed on to the spooler, is sent immediately.



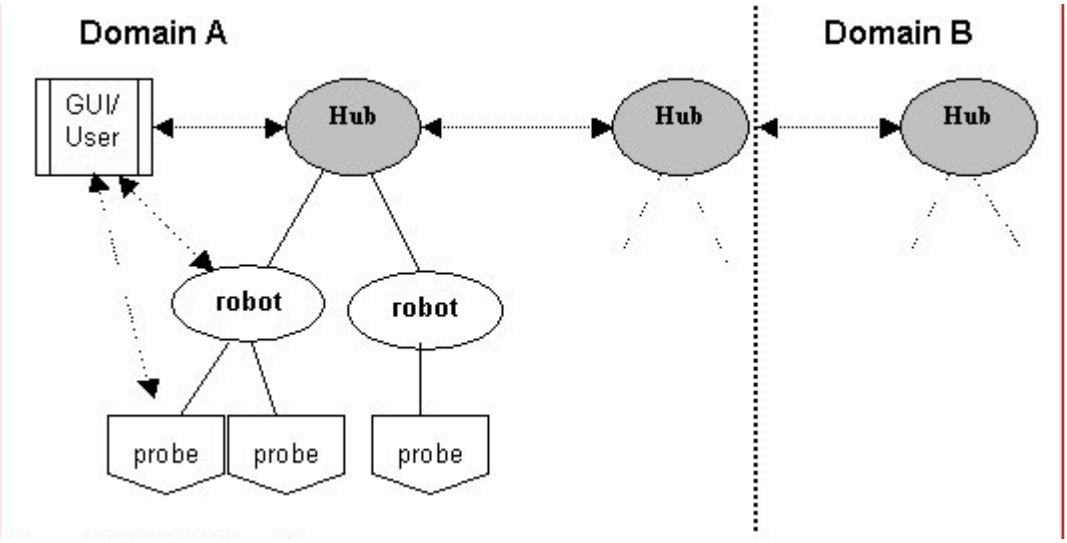
3. The Security Model

This document describes the security models found within the system. Our main security goals are to determine whether to restrict users and/or probes based on predefined permissions within the Domain. The security topics discussed in this document are:

- **Access** who has permission to do what
- **Authentication** is the client who he/she/it claims to be?
- **Encryption** make it impossible for others to read the data

System Overview

The Genesys Monitoring Platform consists of Domains, Hubs, Robots and probes. A typical installation may look like this.



Consider the following scenario:

- A user performs a Login and wants to configure a probe

The security steps involved in the above scenario is explained in detail below:

1. The user performs a login on a Domain with a user name and a password before he can start managing the nodes in the domain. If the login succeeds the user will be granted BHubs that verify the SID's upon request by the controller.

2. The SID is attached to all requests and the node forwards it to the local Robot for verification of the users' permissions. The robot forwards the request to the Hub witch first checks the domain signature and then the users' permissions, and accepts or denies the request.

The Session Identification (SID)

The SID is used to control the users/probes access to execute commands on the appliance . When a client sends a request to a node it must have a valid SID. The SID is issued by the nearest appliance (Domain login) and will require a user name and a password if it is a user or verification from the controller if it is a probe.

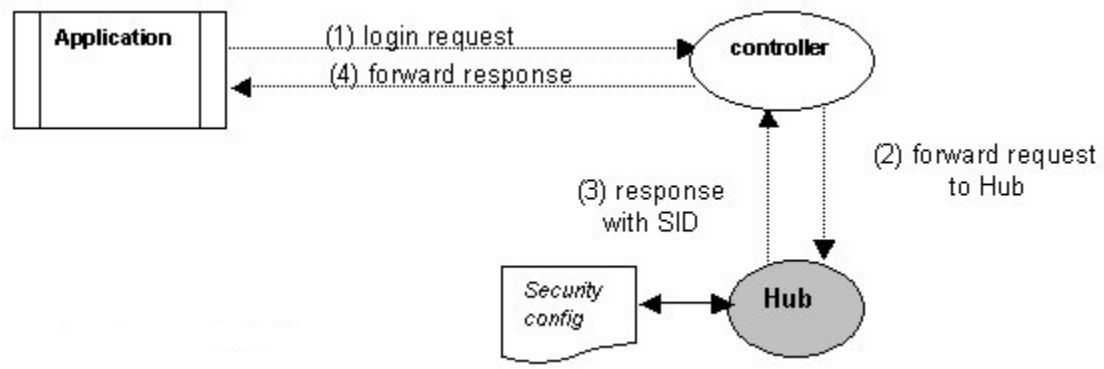
The SID contains the following information:

- Signature (16 bytes) - the signature is based on a password set by the administrator (HMAC)
- Version (2 bytes)

- Expire time (EPOCH)
- Hub (Login)
- Client IP-address
- Client Ethernet address
- Client type (user or probe)
- Client identity (user-name or probe-name)
- The SID is encoded with Base64 to make it easier to transfer between applications.

Login

Login requests are sent from user applications (and probes with special requirements). These requests are checked against the security setup in the appliance . A typical login request is described below:



When a user is logging in, a login request is sent to the controller. The request contains:

- user name
- password

The controller receives the request and forwards it to the appliance after adding the following fields:

- IP address of the source
- MAC address of the source
- The Hub checks the information against the security configuration and sends a reply with a SID if the login request is valid.

Verifying a SID

A node receives a request and asks the controller to verify the SID. The request is forwarded to the appliance hub probe, which verifies the signature of the SID and checks the rest of the information against the access required by the node.

Whenever a request is sent to a probe, the SID for that user is attached. The SID and information about the client is sent to the Hub to check that the user has the access level required to execute the requested command.

The information added by the node is:

- Client IP-address
- Client MAC address
- The commands required access.

The Configuration File

The **appliance** has a security setup file that contains information about the users and probes that have access to the Monitoring Solution and what permissions they have.

The setup section contains generic configuration items such as how long the SID is valid and the signature.

The users section contains user information such as user name, access rights and password. See also the section Access Control Lists (ACLs). The Infrastructure Manager tool uses the profile variable to set the look and feel for the GUI.

The Probes section is used for giving probes access to other probes.

The Filters section can be used to give access-rights to hosts instead of users and *should not be used*.

Please note that this file is monitored with a checksum, so tampering causes the Hub to invalidate the configuration.

Access Control Lists (ACLs)

Access Control Lists consists of a set of access properties and permissions. When the administrator creates new users, or modifies the properties for an existing user, he attaches the user to an ACL. Users attached to an ACL will have the properties and permissions defined for that ACL.

The administrator can also create new ACLs or modify the properties for the existing ones.

The Signature

When a new appliance is added to the domain, the Central Hub detects that there is a new Hub without security enabled in the Domain, and is prompted to manage the unsecured Hub. The signature and the users are distributed to the new Appliance . If the administrator logs on to the new Hub he is forced to login on a secure Hub.

Alarm Solution

The Alarm server (nas) connects to the hub probe located on Central Hub and collects any messages with a subject of Alarm from downstream appliance . These Alarms are sorted and stored in the Alarm Database and then posted back through the Central Hub to the Alarm Sub Console (which is integrated into the Infrastructure Manager and Monitoring Portal.

4. The Appliance

The appliance is the main customer component of the Genesys Monitoring Platform enabling end-users to supply the support organization with current and historical device 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 Appliance is installed in a customer site, where it communicates with multiple devices residing within the same private network (not necessarily at the same location). The appliance performs the following functions:

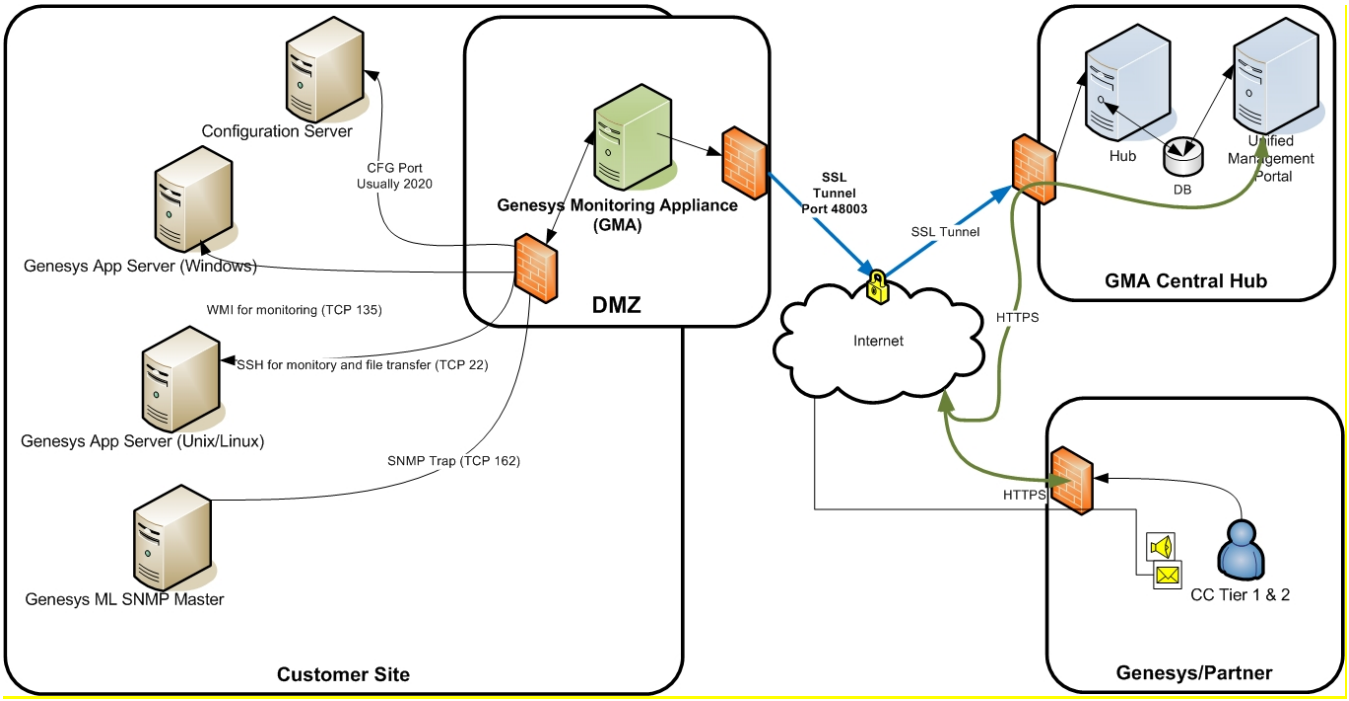
- Periodic and event-driven collection of device data; create and store a history of device data including inventory, status, configuration and performance information, log files, and any other data relevant to support incident handling.
- Execution of command sets on devices, including software upgrades, the results of which are saved as part of the device history.
- Collection of device data when requested by the user, creating a current snapshot of relevant data.
- Proactive collection based on run-time analysis of data.
- Current data is collected by the appliance and transmitted to the Central Hub and stored in the database for viewing via the Portal.
- Automatic creation of reports when collected data (or result data from commands executed on the device) may indicate a problem with the device (optional).
- Automatic creation of reports every time a Collection or Activity Profile is run (optional).
- Automatic transmission of all automatic reports without user interference (optional, and only when permitted by the appliance administrator).
- Enables the support representatives to achieve remote access to any of the devices for support purposes.
- No data can be received from or sent to the Central Hub without the permission of the Appliance administrator. The Central Hub is never granted remote access to any device without the permission of the Appliance administrator.

5. Architectural Considerations

The general architecture has each appliance (Relay Hub) within customer environment connected to the Central Hub via the SSL Tunnel.

Depending on the size of the implementation, Genesys may need to deploy additional Appliances (Relay Hubs) to support the number relay hubs, robots (agents), devices, etc.

This is normally accomplished by allocating a pair of Relay Hubs as Tunnel Servers for the additional downstream Relays to support the additional load.



6. Firewall Requirements

Appliance Communications

- **48003**/TCP: (Outbound only) for the SSL tunnel connection back to Concentrator Hub

  Concentrator Hub IP address 52.42.14.194 port 48003 Monitoring Portal

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

Remote Access (optional)

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

Internal Agent-less Monitoring Communications

- 22/TCP: SSH protocol access to monitored Unix based Genesys Component Servers from the appliance. SSH provides the appliance with a secure way to connect to a Genesys Component Server in order to run monitoring routines. Authentication can be done via RSA keys.
- 135/TCP: WMI protocol access to monitored Windows based Genesys Component Servers from the appliance. WMI allows the appliance to gather the necessary host and component metrics.
- **Configuration Server Port:** (Usually port 2020). Configuration Server port needs to be opened to enable auto-discovery. Auto-discovery allows detecting addion or removal of servers in the environment so they could be added or removed from the monitoring process.
- User account on the Genesys Component Server with limited permissions. This user account provides the security context for monitoring routine execution.

7. SNMP and Other requirements

Appliance Communications

- SNMP Traps from the Genesys Management Layer. These traps alert Genesys Expertsto issues reported by the Genesys management layer.
- SNMP access to the Genesys SNMP Master Agent. SNMP access to the Genesys SNMP Master Agent allows Genesys experts to perform more detailed Genesys application analysis/alerting such as call rate and call volume.
- Remote control to the appliance through the Service Center platform is requested. This allows Genesys experts to maintain and support the appliance itself.

NOTE: Ensure that the SNMP and Genesys SNMP Master agent are enable in the environment and their corresponding licenses are valid. The lack of these components will limit the monitoring capabilities.

Optional Service Requirement

- SCP/SFTP access from the monitored Genesys component servers to appliance as an intermediary step prior to transfer to Genesys Secure FTP server.

Other tools included:

- Auto-discovery – Tool to connect to Configuration Server to discover host and apps changes and apply then to the GMA
- PuTTY
- WMI Explorer
- Process Explorer-requisite software that we install on the appliance that assists in our collections.
- Perl
- Java
- MySQL (optional)
- Net-SNMP
- SNMPTT
- Nimsoft Relay

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 approved Genesys component servers.
- The user account for accessing the Genesys Component server can be a limited privilege user with permissions only to run permitted OS and Genesys commands. This user will also need

read permissions on log file directories and core files if the automated log gathering process is leveraged.
- HTTPS access can be restricted and logged only to the appliance.

SNMP community string can be 'read only' and trap destination restricted to Genesys Monitoring platform. *Note – In order to monitor call rate and volumes Genesys Experts would require SNMP set permissions.

8. Server Requirements

Operational Systems Supported: Currently GMA can be installed on Windows 2008 and Windows 2012 Servers

Deployment size	Physical or virtual server requirements	
	Processor (XEON-class 2.0 GHz or better)	**Memory**
One Relay hub, fewer than 250 robots Modest deployment	One quad-core processor	2 GB to 4 GB
Two to Three Relay hubs, fewer than 500 robots Medium-scale deployment	One or two quad-core processors	2 GB to 4 GB
Two Relay (concentration) hubs, four to six Infrastructure hubs, up to 1000 robots Large-scale deployment	Two quad-core processors	4 GB to 8 GB
Two to Four Relay (concentration) hubs, eight to ten Infrastructure hubs, up to 2000 robots Major deployment	Two quad- or eight-core processors	4 GB to 8 GB
Four or more Relay (concentration) hubs and over ten infrastructure hubs, over 2000 robots	Use the specifications above as a starting point and consult with Genesys.	

9. Communication

The appliance and the Central Hub exchange information through the tunnel using a SSL tunnel which, ensures both authentication and encryption of the data.

Each appliance transmits information to the Central Hub and retrieves information via Genesys Probe (agent-less) or via agents from monitored devices. The appliance runs scripts at set intervals, accept any waiting messages, and then transmit the data collected to the Central Hub for storage in the database.

This method can be used even when firewalls exist, because customers are allowing **48003** outbound and the tunnel client (Appliance) always initiates communication with the Central Hub.

Tunnels

Most companies today have one or more firewalls in their network, both internally between different networks and externally against a DMZ or Internet.

See also the section “Setting up a tunnel between two Hubs that are separated by a Firewall”.

Network administrators are often reluctant to open a firewall for a lot of IP addresses and ports in order to make it possible for Management applications to work. This makes it difficult to administrate and monitor the whole network from a central location.

The solution is to set up a Tunnel between two Hubs that is separated by a Firewall. The Tunnel sets up a SSL (Secure Sockets Layer) connection between the two Hubs and enables all requests and messages to be routed over the Tunnel and dispatched on the other side. This routing will be transparent to all the users within Genesys Monitoring Solution. The only requirement for setting up a connection is that one of the Firewalls opens an outbound port for connection to the target Hub on **one** port, usually 48003.

Security is the main issue when opening a Firewall for external connections. The Tunnel is implemented using the SSL protocol, which is currently the most widely deployed security protocol today (e.g. it is the protocol behind Secure HTTP (HTTPS)). See also the section Encryption. The security is handled in two ways; certificates to authenticate the Client and encryption to secure the network traffic (e.g. over Internet):

Authorization and Authentication

The Tunnel provides authorization and authentication by using certificates. Both the Client and the Server need valid certificates issued by the same CA (Certificate Authority) in order to set up a connection. In the case of setting up a Tunnel, the machine receiving the connection (the Server) is its own CA and will only accept certificates issued by itself.

Encryption

The encryption settings spans from *None* to *High*. No encryption means that the traffic is still authenticated and is therefore recommended for Tunnels within LAN’s and WANs. Selection of higher encryption level will result in higher resource usage for the machines at both ends of the tunnel.

Encryption

The infrastructure supports Open SSL (Secure Socket Layer), thus encrypting the data-channels in the Genesys Appliance.

This excerpt is from the http://www.openssl.org documentation and states the goal for the SSL protocol.

"*The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP[TCP]), is the* ***SSL Record Protocol****. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the* ***SSL Handshake Protocol****, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently.*

The SSL protocol provides connection security *that has three basic properties:*

- *The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES[DES], RC4[RC4], etc.)*
- *The peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA[RSA], DSS[DSS], etc.).*
- *The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations*. "

10. Remote Access

Optional Remote access allows the authorized Genesys Experts to gain access to the appliance and supported devices. From here the Genesys Experts can perform tasks like log capture, appliance troubleshooting, etc. Gaining remote access involves third-party secure access software such as Bomgar or WebEx. In order for remote access to function properly, the appliance requires outbound access to the Bomgar (ts-bomgar-ca.genesyslab.com -198.164.227.30) secure servers via a dedicated SSL tunnel over 443.

Remote access is enabled at installation time when customer security policies permit the use of dynamic SSL tunnels to access their facilities.

11. Extracted Data being Transmitted

Genesys leverages monitoring routines that check Genesys component servers for issues such as CPU, Memory, process information (Genesys solutions), check for core files and disk utilization. These monitoring routines are modular and based on security concerns and component monitoring requests that can be removed or added as desired.

An example of typical deployment monitoring routines:

Genesys Management Layer Traps – The Genesys Management Layer is configured to send all Genesys Management Layer alarms to the Genesys Monitoring Platform

Operating System Commands (Unix)

CPU and Memory

- vmstat - information about processes, memory, paging, block IO, traps, and cpu activity.
- CPU Utilization (via vmstat)
- Number of CPUs (via dmesg or equivalent)
- Memory Utilization (via vmstat)

File Systems

- Get File System Info (via df)

Software Packages

- Get Package List (via rpm or equivalent)

Processes

- Get Process List (via ps aux)
- Get Processes (Long Names) (via ps -ef)

UpTime

- UpTime (via uptime)

Operating System Commands (Windows - WMI)

Some of the queries are:

CPU and Memory

- Select * from Win32_Processor
- Select * from Win32_OperatingSystem

Processes

- select CommandLine, ProcessId, WorkingSetSize from Win32_Process

For more details of the WMI queries please refer to Appendix A.

Genesys Monitoring Commands

Get Process Info

- Get Process Info (Perl script)

Check Core Files

- Checks for presence of Core Files (Perl script)

CME export

- Extracts the CME configuration for Change analysis (Perl script)

12. Appliance Provisioning

The customer 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 stated in the appliance section.

Appliance Access

As far as user account access to the appliance , Genesys is open to follow the customer user creation guidelines be it local accounts, domain accounts, etc. We are open to individual Genesys Experts accounts or a general Genesys (Customer can dictate this based on their security requirements).

13. Genesys Host Accounts Access

There are 2 ways the appliance accesses Genesys Hosts. Unix hosts are accessed from the appliance via SSH (port 22). Windows hosts are accessed from the appliance via WMI (port 135).

Appliance → Unix Hosts	SSH, port 22
Appliance → Windows Hosts	WMI, port 135

The appliance requires an account that can be used to access Unix hosts. Genesys prefers to use a single account with a password that never expires. Genesys essentially needs read-only access to the hosts but must be able to execute the commands described in the *Extracted Data being Transmitted* section. Genesys understands that this may not be possible under the Customer user creation policies and are willing to work with Customer to optimize this issue for both parties.

The appliance requires an account that can be used to access Windows hosts. ***A domain user with privileges to execute the collection commands on all Genesys application server hosts. Further security settings should be discussed with a customer's system administrator in review of the provided WMI commands found in Annex A.***

14. Annex A – WMI Permissions Considerations

To enable WMI monitoring with GMA as part of our standard “Remote Alarm Monitoring – Advanced” deployment, we need a user with permissions that allow us to run the following commands, and return the expected outputs and formats specified below, including the data in the fields. E.g.: Caption=gda.exe

The output can be limited to include only the Genesys applications and processes running on the host, as those are the only ones we monitor. Example: SIP Server, Statserver, WFM, LCA, Java based Genesys processes, etc. If the permissions granted include additional non-Genesys processes in some of the outputs, they will be ignored by our tools.

Setting the WMI Permissions on the server being queried:

Add the non-administrator user(s) in question to the Performance Monitor Users group

- Under Services and Applications, bring up the properties dialog of WMI Control (or run wmimgmt.msc). In the Security tab, highlight Root/CIMV2, click Security; add Performance Monitor Users and enable the options : Enable Account and Remote Enable
- Run dcomcnfg. At Component Services > Computers > My Computer, in the COM security tab of the Properties dialog click "Edit Limits" for both Access Permissions and Launch and Activation Permissions. Add Performance Monitor Users and allow remote access, remote launch, and remote activation.
- You will then need to add “(A;;KA;;;MU)” to the SCMANAGER security description. To do this:
- From an Administrator: Command Prompt, Run: “sc sdshow SCMANAGER” and take the output, example: D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
- Insert “(A;;KA;;;MU)” after the “D:” so it all looks like this: D:(A;;KA;;;MU)(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
- Then take the new string and run this command: “sc sdset SCMANAGER D:(A;;KA;;;MU)(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)”

Note: The examples below are showing the commands and output format expected including the output parameters required (i.e.: “ProcessId”, “Name”, etc.). The value of the output parameters (list of processes, etc.) will vary per server depending on the applications running on it.

1) **WMI Query**: SELECT Name, CommandLine, ProcessId, WorkingSetSize FROM Win32_Process WHERE CommandLine LIKE '%\\[Cc][Nn]\\bin\\%.exe%' OR CommandLine LIKE '%\\[Gg][Cc][Tt][Ii]**Error! Hyperlink reference not valid.**'

Output:

Name=gda.exe

CommandLine="C:\Program Files\GCTI\Local Control Agent\gda.exe" 5000 -service GDA

ProcessId=1256

WorkingSetSize=11931648

Name=lca.exe

CommandLine="C:\Program Files\GCTI\Local Control Agent\lca.exe" 4999 -service LCA64

ProcessId=1332

WorkingSetSize=17350656

2) **WMI Query**: SELECT ExecutablePath, ProcessId, WorkingSetSize, KernelModeTime, UserModeTime FROM Win32_Process

Output:

ExecutablePath=C:\Program Files\GCTI\Local Control Agent\gda.exe

ProcessId=1256

WorkingSetSize=11931648

KernelModeTime=312002

UserModeTime=0

ExecutablePath=C:\Program Files\GCTI\Local Control Agent\lca.exe

ProcessId=1332

WorkingSetSize=17350656

KernelModeTime=3272744979

UserModeTime=24843627253

3) **WMI Query**: SELECT PathName FROM Win32_Service

Output:

PathName="C:\Program Files\GCTI\Local Control Agent\gda.exe" 5000 -service GDA

PathName="C:\Program Files\GCTI\Local Control Agent\lca.exe" 4999 -service LCA64

PathName="C:\Program Files\Genesys\bin\nimbus.exe"

PathName=C:\Program Files\GCTI\LFM\cygwin\bin\cygrunsrv.exe

---

4) **WMI Query:** SELECT Name FROM Win32_ComputerSystem

Output:

Name=CA-TO-ALUM

5) **WMI Query**: SELECT IDProcess, PercentProcessorTime, Timestamp_Sys100NS FROM Win32_PerfRawData_PerfProc_Process

Output:

IDProcess=0

PercentProcessorTime=621291843366492

Timestamp_Sys100NS=131351962115924057

IDProcess=4

PercentProcessorTime=10523983461

Timestamp_Sys100NS=131351962115924057

IDProcess=336

PercentProcessorTime=936006

Timestamp_Sys100NS=131351962115924057

---

6) **WMI Query**: Select Caption, DriveType, FreeSpace, Size, Description, FileSystem FROM Win32_LogicalDisk

Output:

Caption=C:

DriveType=3

FreeSpace=105478909952

Size=598772543488

Description=Local Fixed Disk

FileSystem=NTFS

Caption=D:

DriveType=5

FreeSpace=

Size=

Description=CD-ROM Disc

FileSystem=

7**) WMI Query**: SELECT IPAddress, IPSubnet, DefaultIPGateway, DNSHostName, DNSDomain, MacAddress, DHCPEnabled, Description FROM Win32_NetworkAdapterConfiguration WHERE IPEnabled=TRUE

Output:

IPAddress=ARRAY(0x30bb224)

IPSubnet=ARRAY(0x30bbe94)

DefaultIPGateway=ARRAY(0x30bd0bc)

DNSHostName=ca-to-alum

DNSDomain=

MacAddress=A4:BA:DB:1D:F7:1B

DHCPEnabled=0

Description=Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Client)

8**) WMI Query**: SELECT * FROM Win32_PerfRawData_Tcpip_TCPv4

Output:

Caption=

ConnectionFailures=313

ConnectionsActive=536870

ConnectionsEstablished=111

ConnectionsPassive=509569

ConnectionsReset=752623

Description=

Frequency_Object=0

Frequency_PerfTime=2208076

Frequency_Sys100NS=10000000

Name=

SegmentsPerSec=53985390

SegmentsReceivedPerSec=27953602

SegmentsRetransmittedPerSec=63103

SegmentsSentPerSec=26031788

Timestamp_Object=0

Timestamp_PerfTime=8749992436654

Timestamp_Sys100NS=131351818117790000

9**) WMI Query**: SELECT * FROM Win32_Processor

Output:

AddressWidth=64

Architecture=9

AssetTag=

Availability=3

Caption=Intel64 Family 6 Model 26 Stepping 5

Characteristics=

ConfigManagerErrorCode=

ConfigManagerUserConfig=

CpuStatus=1

CreationClassName=Win32_Processor

CurrentClockSpeed=2261

CurrentVoltage=12

DataWidth=64

Description=Intel64 Family 6 Model 26 Stepping 5

DeviceID=CPU0

ErrorCleared=

ErrorDescription=

ExtClock=5860

Family=179

InstallDate=

L2CacheSize=1024

L2CacheSpeed=

L3CacheSize=8192

L3CacheSpeed=0

LastErrorCode=

Level=6

LoadPercentage=0

Manufacturer=GenuineIntel

MaxClockSpeed=2261

Name=Intel(R) Xeon(R) CPU L5520 @ 2.27GHz

NumberOfCores=4

NumberOfEnabledCore=

NumberOfLogicalProcessors=8

OtherFamilyDescription=

PartNumber=

PNPDeviceID=

PowerManagementCapabilities=

PowerManagementSupported=0

ProcessorId=BFEBFBFF000106A5

ProcessorType=3

Revision=6661

Role=CPU

SecondLevelAddressTranslationExtensions=

SerialNumber=

SocketDesignation=CPU1

Status=OK

StatusInfo=3

Stepping=

SystemCreationClassName=Win32_ComputerSystem

SystemName=CA-TO-ALUM

ThreadCount=

UniqueId=

UpgradeMethod=25

Version=

VirtualizationFirmwareEnabled=

VMMonitorModeExtensions=

VoltageCaps=

AddressWidth=64

Architecture=9

AssetTag=

Availability=3

Caption=Intel64 Family 6 Model 26 Stepping 5

Characteristics=

ConfigManagerErrorCode=

ConfigManagerUserConfig=

CpuStatus=4

CreationClassName=Win32_Processor

CurrentClockSpeed=2261

CurrentVoltage=12

DataWidth=64

Description=Intel64 Family 6 Model 26 Stepping 5

DeviceID=CPU1

ErrorCleared=

ErrorDescription=

ExtClock=5860

Family=179

InstallDate=

L2CacheSize=1024

L2CacheSpeed=

L3CacheSize=8192

L3CacheSpeed=0

LastErrorCode=

Level=6

LoadPercentage=0

Manufacturer=GenuineIntel

MaxClockSpeed=2261

Name=Intel(R) Xeon(R) CPU L5520 @ 2.27GHz

NumberOfCores=4

NumberOfEnabledCore=

NumberOfLogicalProcessors=8

OtherFamilyDescription=

PartNumber=

PNPDeviceID=

PowerManagementCapabilities=

PowerManagementSupported=0

ProcessorId=BFEBFBFF000106A5

ProcessorType=3

Revision=6661

Role=CPU

SecondLevelAddressTranslationExtensions=

SerialNumber=

SocketDesignation=CPU2

Status=OK

StatusInfo=3

Stepping=

SystemCreationClassName=Win32_ComputerSystem

SystemName=CA-TO-ALUM

ThreadCount=

UniqueId=

UpgradeMethod=25

Version=

VirtualizationFirmwareEnabled=

VMMonitorModeExtensions=

VoltageCaps=

10) **WMI Query**: SELECT PercentIdleTime, PercentInterruptTime, PercentPrivilegedTime, PercentProcessorTime, PercentUserTime FROM Win32_PerfFormattedData_PerfOS_Processor where Name='_Total'

Output:

PercentIdleTime=93

PercentInterruptTime=0

PercentPrivilegedTime=0

PercentProcessorTime=8

PercentUserTime=6

11) **WMI Query**: SELECT * FROM Win32_PerfFormattedData_PerfOS_System

Output:

AlignmentFixupsPerSec=0

Caption=

ContextSwitchesPerSec=1260

Description=

ExceptionDispatchesPerSec=0

FileControlBytesPerSec=6224

FileControlOperationsPerSec=285

FileDataOperationsPerSec=0

FileReadBytesPerSec=0

FileReadOperationsPerSec=0

FileWriteBytesPerSec=0

FileWriteOperationsPerSec=0

FloatingEmulationsPerSec=0

Frequency_Object=

Frequency_PerfTime=

Frequency_Sys100NS=

Name=

PercentRegistryQuotaInUse=6

Processes=80

ProcessorQueueLength=0

SystemCallsPerSec=601711

SystemUpTime=3962846

Threads=1067

Timestamp_Object=

Timestamp_PerfTime=

Timestamp_Sys100NS=

12) **WMI Query**: select FreePhysicalMemory, FreeSpaceInPagingFiles, FreeVirtualMemory, MaxProcessMemorySize, SizeStoredInPagingFiles, TotalVirtualMemorySize, TotalVisibleMemorySize from Win32_OperatingSystem

Output:

```
----------

FreePhysicalMemory=9973388

FreeSpaceInPagingFiles=12552192

FreeVirtualMemory=21590428

MaxProcessMemorySize=8589934464

SizeStoredInPagingFiles=12572760

TotalVirtualMemorySize=25143676

TotalVisibleMemorySize=12572760
```

13) **WMI Query:** select * from Win32_PerfRawData_PerfOS_System

Output:

```
----------

AlignmentFixupsPerSec=0

Caption=

ContextSwitchesPerSec=-1151992891

Description=

ExceptionDispatchesPerSec=168243

FileControlBytesPerSec=11727403880

FileControlOperationsPerSec=600488353
```

FileDataOperationsPerSec=-1386007487

FileReadBytesPerSec=122438149250

FileReadOperationsPerSec=36263219

FileWriteBytesPerSec=147875755772

FileWriteOperationsPerSec=-1422270706

FloatingEmulationsPerSec=0

Frequency_Object=10000000

Frequency_PerfTime=2208076

Frequency_Sys100NS=10000000

Name=

PercentRegistryQuotaInUse=145404880

Processes=80

ProcessorQueueLength=0

SystemCallsPerSec=808006179

SystemUpTime=131312333675811966

Threads=1067

Timestamp_Object=131351962144940108

Timestamp_PerfTime=8749998443018

Timestamp_Sys100NS=131351818144940000

14) **WMI Query**: SELECT Caption, ProcessId, WorkingSetSize FROM Win32_Process

Output:

Caption=gda.exe

ProcessId=1256

WorkingSetSize=11931648

Caption=lca.exe

ProcessId=1332

WorkingSetSize=1735065