GENESYS™

# PURECONNECT CLOUD CUSTOMER HANDBOOK

This handbook is revised periodically as we improve our processes and respond to customers' needs. Please check our web site (https://mycloud.inin.com/terms-and-conditions) for the most current handbook.

Information contained within this document is subject to change without notice and not approved for general circulation. This document may NOT be disclosed to third parties unless a NDA has been executed between Genesys and recipient party.

| Name | Modification | Date |
|---|---|---|
| **Zach Hinkle** | Initial release v1.1 | 7/23/14 |
| **Zach Hinkle** | 2.0 | 12/15/14 |
| **Zach Hinkle** | 2.1 | 1/30/15 |
| **Zach Hinkle** | 3.0 | 5/14/15 |
| **Zach Hinkle** | 3.1 | 11/19/15 |
| **Bill Dummett** | 4.0 | 03/05/17 |
| **Nikki Kisor** | 4.1 | 05/25/17 |
| **Joe Hynes** | 4.2 | 11/03/17 |
| **Nikki Kisor** | 4.3 | 1/11/2018 |
| **Nikki Kisor** | 4.4 | 3/20/2018 |
| **Nikki Adams** | 4.5 | 8/8/2018 |
| **Nikki Adams** | 4.6 | 9/10/2018 |

7601 Interactive Way
Indianapolis, IN 46278

# Contents

# PureConnect Cloud Mission Statement

PureConnect Cloud, a world class service of the Genesys Telecommunications Laboratories, Inc. ("Genesys") solution, provides the feature set, tools, support, and assistance necessary to enable customer success.

# Customer Guide Purpose

This document provides our customers with an overview of how the service is designed, maintained, and provided on a daily basis. Upon reading this document, customers should have a better understanding of the service and teams that are responsible for delivering their contact center solution.

# Service Overview

Your cloud contact center solution is designed, developed, tested, maintained, operated, and supported by Genesys. Our service offering relieves your teams of the burden to operate, manage, and secure the life cycle management of your contact center solution. Our offering is delivered to your business from geographically redundant data centers to provide business continuity and disaster recovery. We provide your organization with the ability to receive, route, and deliver to your customers inbound multimedia interactions. We can also provide your organization with industry leading outbound dialing functionality.

# Guiding Principle

Your service is delivered from secure hardened data centers with co-location facilities. Each data center complies with the following:

- State of the art physical security comprised of 24x7 manned security desks, biometric scanning, and/or electronic key-card access controls
- Annual SSAE 16 Type II Review
- Redundant UPS, generator service, and environmental cooling units
- Designed to withstand sustained wind gusts of up to F3, on the Fujita Scale

Your live production use of our service is continually monitored 24/7/365 by our Network Operations Center (NOC). Your delivery components are routinely backed up, and we also offer hardware maintenance contracts with replacements for all critical components- whether they reside in our data centers or your premises.

# Service Editions

Beginning September 1st, 2018, Standard, Preferred, and Premium editions have been consolidated and will no longer be available to upgrade to.  Existing customers may continue to add seats based on their current edition.  However, at contract renewal or if increased functionality is needed, then the upgrade path will be to the Enterprise Edition.

- **Standard** – Available for agent counts of 25 up to 500 users. Base functionality includes ACD, IVR, and UC capabilities. Available options include multichannel (voice, email, and chat), speech recognition, voice recording and quality management, workforce management, real time speech analytics, post-call and IVR surveys, select CRM and UC integrations, supervisor and reporting capabilities.
- **Preferred** – Available for agent counts of 25 up to 5,000 users. Designed for organizations seeking extended options to deliver more advanced contact center functionality. The Preferred Edition includes all the Standard Edition capabilities and additional options, including: outbound dialing, web portal for outsourcers, agents and management, screen recording, strategic resource planning, additional media channels, a broad set of packaged integrations, the ability to write custom integrations to our public API, and business process automation capabilities.
- **Premium** – Available for agent counts of 25 and beyond 5,000 users. The Preferred Edition allows for advanced options such as: natural language speech recognition, VoiceXML, advanced text to speech and enhanced customization.

- **Enterprise Edition** – Allows for all services and capabilities offered on PureConnect Cloud

## Base Service Offering

Our service offering relieves your teams of the burden to operate, manage, and secure the life cycle management of your contact center solution. Geographically redundant PureConnect servers deliver each edition of our service. Should a catastrophic event occur at one of our regional service data centers the backup server, located in the secondary data center, will assume primary responsibility for delivering your service. Our service deliverables are divided in the following categories:

| Service Type A: ACD and IVR Telephony | Service Type B: Enterprise Telephony | Service Type C: Multimedia Interactions | Service Type D: Administrative Apps | Service Type E: Ancillary Services |
|---|---|---|---|---|
| - Routing<br>- Priority<br>- Queue Assignment<br>- Call Recording | - Routing / Switching<br>- Ad-hoc Recording<br>- Ad-hoc Conferencing | - Email<br>- Web Chat (customer hosted)<br>- Callbacks<br>- Dialer<br>- SMS<br>- Generic Objects<br>- Fax | - Administrator<br>- Attendant<br>- Business Manager<br>- Interaction Supervisor | - Interaction Web Portal<br>- Web Servers<br>- VXML Interpreters<br>- TTS / ASR<br>- Genesys WFM<br>- Genesys Interaction Analytics |

- **Service Type E –** The feature offerings are facilitated by applications that are not inherently switchover (hot/active standby) capable, or are not offered redundantly by default. Redundancy, delivered geographically, can be purchased but may not be delivered in a hot/active standby configuration.
- **Business Continuity (BC)** – Our ability to supply your purchased services irrespective of a single point of failure.
- **Disaster Recovery (DR)** – Our minimum commitment for duplication of your purchased services in the event of a catastrophe in a single service data center. Our DR commitment consists of the activation and/or deployment of a pre-existing, off-site backup of vital configuration, and historical information in a new physical infrastructure that includes all relevant service components.
- **Recovery Point Objective (RPO) –** The maximum period of time in which data might be lost from a catastrophic event at a single service data center.
- **Restoration Time Objective (RTO) –** The maximum duration of time to restore services after a catastrophic event at a single service data center.

### Business Continuity Matrix

Each edition of our service is provided by geographically redundant PureConnect servers to provide BC for each of the service delivery types listed below:

| PureConnect Cloud Model | Business Continuity - Primary Data Center (Services Type) | | | | | Business Continuity - Secondary Data Center (Services Type) | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **A** | **B** | **C** | **D** | **E** | **A** | **B** | **C** | **D** | **E** |
| **Local Control (LCM)** | X | X | X | X | X[1] | X | X | X | X | X[1] |
| **Remote Control (RCM)*** | X | X | X | X | X[1] | X | X | X | X | X[1] |
| [1] | Business continuity requires an additional infrastructure purchase | | | | | | | | | |

** Geo Redundant RCM service customers* ***must*** *have incoming and outgoing calls setup with automatic failover (delivered by default with Genesys provided circuits).*

## Disaster Recovery Matrix

Each edition of our service is provided by geographically redundant PureConnect servers to provide DR for each of the service delivery types listed below:

| PureConnect Cloud Model | Disaster Recovery Mode (Services Types) | | | | | | |
|---|---|---|---|---|---|---|---|
| | RPO | RTO | A | B | C | D | E |
| **Local Control** | 4 Hours | 15 Min | X | X | X | X | X[1,2] |
| **Remote Control*** | 4 Hours | 15 Min | X | X | X | X | X[1,2] |
| [1] | Business continuity requires an additional infrastructure purchase | | | | | | |
| [2] | Excluded from RTO's | | | | | | |

** Geo Redundant RCM service customers **must** have incoming and outgoing calls setup with automatic failover (delivered by default with Genesys provided circuits).*

# Virtual Private Cloud (VPC)

Our service is delivered to your organization via a dedicated instance of PureConnect built on a Virtual Private Cloud (VPC). Your VPC is made of a segmented physical and logical infrastructure components within a larger cloud network that offers you data isolation and security from other service customers.

## VPC Infrastructure Components

- **Tier 3 Data Centers** – Each service data center is a compliant Tier 3 data center. Tier 3 compliance, among other things, means the data center can operate indefinitely without commercial power.
- **Server Instances** – Your service is provided by dedicated application servers (physical or virtual) commonly referred to as multi-instance. Your agent size and application requirements determine physical or virtual server assignment.
- **Network Security –** Connectivity, via a WAN connection, to our service data centers is secured by a dedicated firewall context and dedicated VLAN within our core infrastructure.
- **Data** – Your application data (call history, quality management data, and so on) is stored in an individual database instance in our shared infrastructure. Data security is a top priority of our service offering. Our service operationally adheres to SSAE-16 processes and procedures to provide trusted security of your data. Visit https://www.genesys.com/inin/about/security for more information.
- **Storage** – Logical separation is used to separate your recordings (call and screen) from other customers within our high availability storage servers. By default, these recordings are secured using 256-bit AES encryption with individual private keys. Customers also have the option of storing recordings locally on their own networks.
- **Backups –** Your application servers, stored recordings, and historical data are backed up on a regular basis.
- **Virus Protection** – Your application servers are protected with Anti-Virus software that is updated regularly.
- **NOC Monitoring** – All service infrastructure (servers and networking devices) are monitored 24/7/365 by our Network Operations Center (NOC).
- **Security Measures** – The following security measures are also deployed by default: Intrusion Detection System (IDS), Vulnerability Scanning, and Penetration Testing.

## PureConnect Cloud VPC Advantages

- **Isolation –** Your VPC is isolated from every other service customer.
- **Infrastructure Redundancy –** By leveraging scalable infrastructure equipment, our services are designed for high resiliency and application availability.
- **Maintenance Events –** Multi-instance architecture allows our service operations group to schedule maintenance events at your convenience and timetable.

- **Data Security –** Your data (call history, quality management data, and so on) is housed within a siloed infrastructure**.**
- **NOC Monitoring –** Each infrastructure component responsible for the delivery of your service is monitored 24/7/365 by a fully staffed Genesys Operations team.

## Operational Teams

Your service is deployed, maintained, and managed by the following Service teams: Delivery, Support, and Security. Each team plays an integral part in how your service is provided. A brief description of each of the teams and sub-teams are detailed below.

### Delivery Team

Our Service Delivery team focuses on our architecture, implementation, add-on services, and the ongoing management and maintenance of your service. This team is made up of solution architects, project managers and system engineers.

- **Architecture –** This team of engineers focuses on how your purchased features are designed, implemented, and delivered.
- **Project Management –** This team facilitates the deployment of your service from the initial kick-off meeting throughout customer acceptance of the solution.
- **Infrastructure –** This team works to ensure our global cloud infrastructure is stable, properly maintained, and adheres to our security, regulatory, and compliance obligations. This team focuses on the following:
    - **Systems Maintenance** – Routine maintenance, break/fix of components, and life cycle management of all core infrastructures.
    - **Change Management** – All changes made to our service supporting components (applications, servers, and infrastructure) are documented in accordance with our change management policy. Our Change Advisory Board (CAB) approves changes prior to execution on production system components.
    - **Backups** – All systems and databases are backed up regularly.
    - **Vulnerability Monitoring** – All external facing systems undergo monthly vulnerability scanning to identify potential security risks. Any identified risks are reviewed by the Security and Operations team and remediated.
    - **Patch Management** – As system patches are released from our vendors they are reviewed by our Security and Infrastructure teams and then classified based upon risk. Based on the classification, the patches are systematically deployed to all systems within our service management domain.

### Global Support Team

Our support team provides assistance from 'how to' types of questions all the way to software defect issues. This team is focused on ensuring your service is reliable and properly functioning. Our global team consists of the following types of resources:

- **Support Engineers –** This team provides a one-stop shop for technical support questions and issues.
- **Service Managers –** This team engages with customers from service implementation to production use of our service. Each PureConnect Cloud customer is assigned a Technical Account Manager when services are purchased. The TAM provides the following services for customers:
    - **Support Transition** – Coordination from the Technical Account Management team to the Support team.
    - **Service Management –** Management of your success using our support and services.
- **Network Operations Center (NOC) –** Our NOC utilizes a variety of industry standard monitoring applications to remotely observe and automatically alert on service impacting issues 24/7/365. This team of engineers also performs many of the standard maintenance events as well.
- **Services –** This team has two roles: small projects and software upgrades.

    - **Small Projects –** The primary role of the team is to assist PureConnect Cloud customers with small projects typically less than 40 hours of engineering, design, and implementation. This team is designed to be agile to react quickly to your requests. Typical small projects include:
        - **New Service Configuration –** Configuration of new services such as email routing, web chat, post-call surveys, and so on.
        - **IVR/Auto Attendant Work –** Adjustment to existing configurations within Interaction Attendant® call flows, and the deployment of new IVR call flows.
    - **Software Upgrades –** These include core release updates to PureConnect and related components as well as release patches.

## Security & Compliance

The Security & Compliance team's mission is to protect and preserve the integrity and confidentiality of your data. Below is a list of certifications our service maintains:

- **International Standards Organization (ISO) 27001**
    - Establishment of an Information Security Management System (ISMS)
- **International Standards Organization (ISO) 9001**
    - Establishes the requirements of a Quality Management System (QMS)
- **Statement of Standards for Attestation Engagements (SSAE) 16 Service Organization Control (SOC) Type 2**
    - Cloud security, availability, processing Integrity, confidentiality, and privacy
- **Payment Card Industry (PCI) Data Security Standards (DSS) 2.0 (United States only)**
    - Encryption, vulnerability management program, strong access control, monitoring & testing networks, and information security policy
- **EU-U.S. and Swiss-U.S. Privacy Shield Framework**
    - Notice, choice, onward transfer, security, data integrity, access, and enforcement

Definition, monitoring, and management of applicable regulations and standards are facilitated by the following mechanisms:

- **Information Security Management System (ISMS)** – Our security program that defines policies, process, procedures, and training.
- **Access Control** – Managed access to all system, application, and infrastructure components that provide our services defined in our established Roles Based Access Control (RBAC) list.
- **Data Classification** – Our service has defined information security handling guidelines. Data that is generated is consistently protected throughout its lifecycle in a manner commensurate with its sensitivity level. Data classification matrices are constructed and reviewed annually by the Compliance team.
- **System Hardening** – Security scanning was performed on our base OS images, and the security policies, within our environment to ensure that our core systems are appropriately hardened against cyber-attacks (virus, trojans, worms, malware, and so on).
- **Incident Response & Evidence Preservation** – Process for how the entire organization will respond to a potential security incident. The incident will be communicated, investigated, validated, and remediated. This includes any external notifications to customers. In the case of a determined security incident, all system and log evidence will be collected and cataloged as required by our Security team.

## Data Retention

Historical data is collected as a result of normal contact center operations and PBX functionality. The following are the most common data types collected:

- Voice Recordings
- Screen Recordings
- Historical Call Detail Records
- IPA Records

Other data types are recorded with normal operations (example: system logs, FBMC, and so on). For example, logging will be utilized as necessary to ensure smooth operations and will be managed independently.

### PureConnect Cloud Data Storage Infrastructure

Applicable data is stored in primary storage via a Storage Area Network (SAN) configured in a Redundant Array of Independent Disks (RAID), 6 volumes configuration. This data is backed up in real time to a redundant SAN in the same RAID 6 configuration within the same data center. Each customer's database is also replicated, via SQL log shipping, to the geographically redundant data center each hour. Customers may opt out of database replication to the backup data center if requested.

### Default Retention Periods

| Data Type | Default Retention Periods | | | |
|---|---|---|---|---|
| | **Standard** | **Preferred** | **Premium** | **Enterprise** |
| Voice Recordings | 1 GB per Recorder Add-on[1] | 2 GB per Recorder Add-on[1] | 4 GB per Recorder Add-on[1] | 4 GB per Recorder Add-on[1] |
| Screen Recordings | | | | |
| Interaction Detail Records | 400 Days or 20 GB[2] | 730 Days or 50 GB[2] | 1095 Days or 100 GB[2] | 1095 Days or 100 GB[2] |
| IPA Records | 90 Days | 90 Days | 90 Days | 90 Days |

At 92% utilization with 100% voice recording, 1 GB will be between 35 and 45 days of voice recordings. Stored amounts (measured in GB) greater than listed will be billed at the contracted GB per month price.

[1] *Voice and screen recordings are not typically stored within service data centers for LCM customers*

[2] *Unless retention periods are specifically requested to be extended, your records will be deleted after the specified number of days or once the size limit has been reached whichever comes first.*

### Adjusting the Retention Period

Your data retention period can be adjusted during the implementation phase or during live production. Requests to alter the default retention period when your service is in production will be billed at your contracted MAC rate. Any alteration to the default data retention policy may result in additional storage to be billed at your contracted cloud storage rate. Please see your **Services Order** for more details on cloud storage pricing.

## Data Access

Your historical records database (interaction detail records for calls, emails, chats, and so on) is collected as a result of your use of our service. We provide a variety of methods for you to access historical data. By default, we provide Interaction Center Business Manager (ICBM) and Interaction Report Assistant to provide you access to our standard suite of reports as well as your own custom reports (if deployed). We also provide two (2) alternative options for data access: Raw Data Export and a dedicated Reporting Database.

Upon request, we will provide a nightly export of your full production historical database. Exports are provided in a standard SQL backup format only to our hosted FTP server. Each nightly export is available for 24 hours after posting to our FTP server. Retrieval, importation, and management of this data are your responsibility on your own infrastructure. Importation of our SQL exports requires that your database match, or is updated, compared to our current production version of SQL Server. Please open a support case to request a nightly export.

An additional offering is available for a single read-only dedicated reporting database, which provides Object Database Connectivity (ODBC) access. This database will be updated hourly via SQL log shipping, which provides a mirrored copy of the production database. This offering is available in the Preferred, Premium, and Enterprise editions of our service. Setup fees and Monthly Re-occurring Costs (MRC) apply.

| | | | | |
|---|---|---|---|---|
| PureConnect Cloud Reporting Intervals (15 min interval) | 0:00 | 0:15 | 0:30 | 0:45 |
| Available Time for Query Execution (Date delayed 1 hour) | 0:12 | :010 (+1 hour) | - | - |

# Education Requirements and Options

Customer's staff members will be required to be certified in order to access Genesys' Support department. Genesys offers a wide selection of educational offerings to help you achieve the greatest benefits from our service. Each edition of our service is associated with a variety of web-based educational videos and instructor led web-based training. In addition, our Education department offers a variety of in-classroom offerings including certification on PureConnect. This section of the handbook covers the various educational offerings available.

The PureConnect Cloud Just In Time (JIT) consists of short and concise 1-3 minute voice-guided videos on how to perform a variety of tasks within the platform, triage issues, and work with Support. Each instructor guided video focuses on a singular task and provides quick 'how-to' assistance. Our JIT library is available, without login, to all PureConnect Cloud customers located here: MyCloud Educational JIT Video's. We have JIT videos on the following topics:

| | | | |
|---|---|---|---|
| User Administration | ACD Basics | IC Business Manager | Reporting |

Instructor led web-based training courses are 90-minute webinars that provide a great opportunity to see the latest in Genesys technology. Whether the staff member is a business decision maker, a contact center supervisor, IT manager or agent, webinar attendees will have the ability to run through virtual lab simulations to gain hands-on experience. All introductory webinars are complimentary.

| | |
|---|---|
| **All Editions of PureConnect Cloud** | |
| **Included:**<br>Interaction Client – .Net Edition (90 min)<br>Interaction Client – Web Edition (90 min)<br>Interaction Client - .Net Edition<br>Advanced Options (90 min)<br>Interaction Attendant (90 min)<br>User Management (90 min)<br>Interaction Reporting (90 min) | **Included, if purchased:**<br>Interaction Dialer (90 Min)<br>Interaction Feedback (90 min)<br>Interaction Optimizer (90 min)<br>Interaction Recorder (90 min)<br>Interaction Supervisor (90 min)<br>**In classroom offerings - Available for purchase:**<br>Interaction Administrator (3 days)<br>Interaction Attendant (3 days) |

The PureConnect Cloud Certified Professional certification is based on the PureConnect Cloud Operational Readiness Education (PCORE) curriculum consists of three (3) main categories in the curriculum: administration of the PureConnect Cloud platform, call flow configuration, and support of the platform. Study materials for certification are located on our MyCloud portal (Link). All material is online and self-paced for customers looking to certify their staff. The certification exam will be free of charge to existing PureConnect Cloud customers. Once certified, staff members are also provided access to https://genesyspartner.force.com/customercare/ with their unique login credentials. This site provides staff members with product, support, best practices documentation and the ability to open up Support cases.

Our Support department regularly hosts webinars on troubleshooting and working with Support. For a complete listing of upcoming webinars please visit: https://my.inin.com/products/selfhelp/Webinars/Pages/2015-Support-Webinar-Series.aspx. Archived webinars can be found here: https://my.inin.com/products/selfhelp/Webinars/Pages/default.aspx.

For a complete list and schedule of available courses and other offerings, please visit Genesys' Education Services listing located on our web site at: https://help.genesys.com/resource-center-cic.html.

# Customization Options

The ability to customize your contact center solution is available within all editions of PureConnect Cloud via a variety of options. We offer the ability to create custom handlers, custom database tables, and custom applications. This section details our functionality and requirements for each of our offered options.

## Custom Handlers

Your PureConnect offers a toolkit of logical steps to perform a variety of operations to deliver contact center functionality. Programmatic collections of these tool steps are referred to as 'handlers'. PureConnect's 'system handlers' perform interactions (calls, email, chats, and so on) treatment such as ACD routing, delivery, and disposition. Custom handlers can be created to enhance PureConnect functionality using Interaction Designer®. Custom handlers are approved for use in all editions of PureConnect Cloud.

Custom handlers are defined as any handlers not part of the standard PureConnect offering. Custom handlers can include customization points, custom subroutines, event initiated monitored handlers, and timer initiated handlers. Modified system (or base) handlers are strictly prohibited within PureConnect Cloud.

### Custom Handler Guidelines

- Custom handlers should be avoided in favor of out-of-box functionality or alternative tool sets. However, Genesys recognizes that custom handlers may be needed to enhance the PureConnect Cloud Service offering.
- Custom handler solutions must reduce the overall complexity of the system or enhance functionality of Genesys products contracted by the customer.
- Custom handlers must be designed such that regular code changes (handlers publish) are not required to administer the solution. Any points within a custom handler that a customer desires to make administrative changes to should be configurable via Interaction Administrator® or another Genesys application interface.
- Custom handler solutions must not replicate product functionality offered by Genesys such as Interaction Dialer®, Interaction Web Portal™, and so on.
- Custom handler solutions must be designed to mitigate the risk of handler failures due to common issues (i.e. data corruption, loops, timeouts, and so on).

### Development Requirements

All custom handlers must be developed and tested in a non-production PureConnect environment before publishing to your production PureConnect Cloud environment.

### Interaction Designer in PureConnect Cloud

Access to Interaction Designer for your service is strictly limited to non-production environments. Individuals requesting access must have successfully completed the Interaction Center Handler Developer (ICHD) certification course offered by Genesys Education Services.

Your staff may access Interaction Designer at any time to write, test, or debug custom handlers in non-production environments.

The following Interaction Designer tools are strictly prohibited for use within PureConnect Cloud: Host Interface, Icon, Multi-Site, Interaction Director®, and File I/O (with the exception of Get File Statistics).

### Documentation Requirements

All custom handlers published in your PureConnect Cloud environment must state the name of the individual, company they represent (if development is outsourced), a summary of the handler's purpose in the initiator notes, per custom handler, and corresponding documentation. All documentation must:

- Follow PureConnect Cloud approved documentation templates (open a support case for the latest template) and be submitted to the Genesys Project team and/or PureConnect Support prior to publishing in the customer's production environment.
- Include a baseline test plan for validating core business functionality for use during system upgrades and other maintenance that may affect the custom handler solution.
- Include design steps taken and test cases executed to mitigate the risk of handler failures due to common issues (i.e. data corruption, loops, timeouts, and so on).
- Include proof of testing execution should be submitted to PureConnect Support and retained for audit purposes.

### Service Level Agreement (SLA)

Custom handlers created by your staff are not covered by the PureConnect Cloud SLA agreement and are not eligible for outage credits.

### Release Upgrades

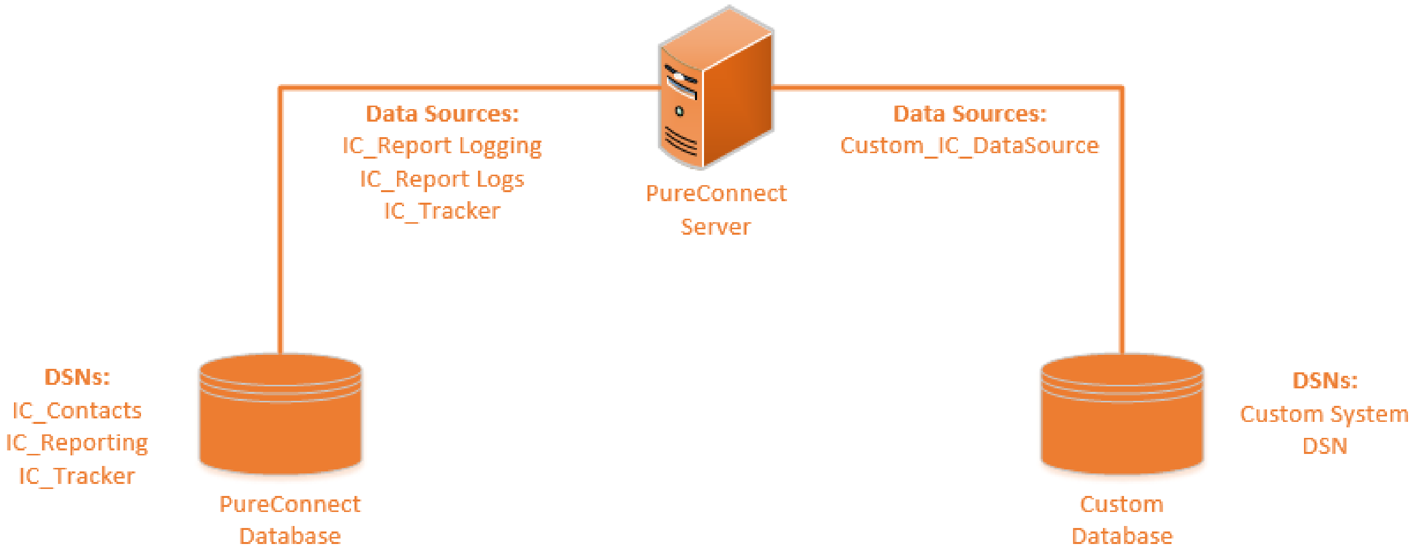
Custom handlers are not evaluated as part of release upgrades, however they are republished as a part of the upgrade. If any additional services work is needed to upgrade a custom handler to the next Release Update or major version it will be at your expense.

## Custom Reporting in PureConnect Cloud

Custom reports are available to be developed and deployed with your service. PureConnect Cloud does support the use of custom tables, custom views, and custom database jobs. Custom tables, within PureConnect Cloud, are **only** supported in a secondary database. Custom stored procedures may be run against the production database, but all result sets are only supported in custom database and associated tables. To utilize this functionality in PureConnect Cloud the following components are required:

- Custom database
- Custom data source in Interaction Administration (PureConnect Cloud provides and handles the implementation task)
- Custom system DSN that points to the custom database

The data source will allow the PureConnect server to communicate with the customized database for reporting on custom tables, views, and stored procedures as well as accessing custom contact lists. The custom system DSN will allow Interaction Attendant® and handlers to communicate with the customization database.



*Note: The customization database will have logins for IC_Admin, IC_User, and IC_ReadOnly. These accounts will provide the necessary access for handlers, reporting, and contact list management.*

### Custom Database Implementation Tasks

If developed by your staff, or an outside partner, the developer is responsible for providing the following items to implement and utilize a custom database:

- Prepare the 'creation script' for the custom database along with the table(s), view(s), or store procedure(s)
- Provide detailed documentation on the purpose and use of the custom database and tables

PureConnect Support will implement and provide support for all approved requests during the implementation and normal service operations. Post implementation phase requests for custom database creation should be opened as Support cases with PureConnect Support.

## Custom Applications

Custom applications are common with our service. You, or an outsourced partner, are able to provide development services for items such as middleware, web services, and IceLib based applications. Custom applications developed do have the following restrictions:

- PureConnect Cloud will not provide any hosting services for customer developed or partner developed applications regardless of service delivery model
- PureConnect Cloud does not currently monitor customer or partner developed custom applications
- PureConnect Cloud Service Level Agreements (SLA) do not apply to customer or partner developed applications
- The developing party is responsible for break / fix support for their developed applications

# Service Delivery Models

## Local Control Model (LCM)

This delivery model requires customers to host some infrastructure components used to deliver service. The following managed and maintained components could be required to be deployed on a customer's premises: Interaction Media Server$^{TM}$, SIP Proxy, Gateway, and Remote Content Server (RCS). Local components allow customers to keep all voice traffic, recordings, and screen recordings locally on the customer's premises.

| | |
|---|---|
| **LCM Characteristics** | |
| **Customer-controlled Hardware Components** | Hardware on Customer's site(s) or any hardware controlled by Customer in Genesys' data centers, including but not limited to: IP phones, local PCs, carrier equipment (MPLS), Media Servers, SIP Proxies, Remote Content Servers (RCS) and voice gateways |
| **Customer-controlled Hardware Maintenance** | Customer is responsible for software or hardware maintenance other than the Genesys proprietary software (examples: operating system, antivirus, etc.) on Customer-controlled hardware. Customer must ensure all Customer-controlled hardware is compatible with all new versions of the Genesys proprietary software. |
| **Telephony Circuits** | Customers utilize their existing telephony lines, existing SIP trunks or purchase new telephony circuits. |
| **Voice traffic** | All voice traffic (RTP) stays local to the customer's network while SIP and other minimal bandwidth traffic flows to the PureConnect Cloud data centers. |
| **Recordings** | Recordings are stored long term in the customer's storage servers by default. |
| **Remote site expansion** (Basic call routing and enterprise telephony) | Two options: 1. Extend an MPLS or Remote VPN Access (RVA) connection to each new site along with Gateways, Media Servers, etc. 2. Connect each new site to the customer's corporate network and route voice over their WAN to the remote site. |
| **Remote survivability** | Yes, by default – The on-site SIP Proxy provides enterprise telephony and basic call routing. |
| **Application Connectivity** | |
| **Type** | **Requirement** |
| Desktop applications – Interaction client - .Net edition and Interaction Center Business Manager (ICBM) | Connectivity to PureConnect Cloud must traverse the private MPLS or RVA connection. Connectivity to the customer's network is required. |
| Terminal Services Remote Applications (TSRA) – Interaction Administrator, Interaction Attendant and ICBM | Connectivity to PureConnect Cloud is provided via the public internet. |
| Web applications | Connectivity to PureConnect Cloud is provided via the public internet. |

## Remote Control Model (RCM)

This delivery model does not require customers to host infrastructure components on their premises. All application infrastructure components are provided within the Genesys data center facilities. Customers are only required to host carrier equipment to facilitate MPLS connectivity to our data centers.

| | |
|---|---|
| **RCM Characteristics** | |
| **Customer-controlled Hardware Components** | Hardware on Customer's site(s) or any hardware controlled by Customer in Genesys' data centers, including but not limited to, IP phones, local PCs, carrier equipment (MPLS), media servers, SIP proxies, Remote Content Servers (RCS) and voice gateways. |
| **Customer-controlled Hardware Maintenance** | Customer is responsible for software or hardware maintenance other than the Genesys proprietary software (examples: operating system, antivirus, etc.) on Customer-controlled hardware.  Customer must ensure all Customer-controlled hardware is compatible with all new versions of the Genesys proprietary software. |
| **Telephony Circuits** | Telephony circuits, Genesys provided or customer provided, are terminated in PureConnect Cloud data centers for local data center media processing (recordings, voice mail, call analysis etc…). Customers are required to purchase fully redundant circuits for the primary and the secondary PureConnect Cloud data centers to ensure for failover capabilities. |
| **Voice traffic** | All voice traffic (SIP and RTP) originates in PureConnect Cloud data centers then traverses the private WAN connection to the customer's network for termination. |
| **Recordings** | Recordings are stored in PureConnect Cloud data centers by default, but can be stored locally as well. |
| **Remote site expansion** | Two options: 1. Extend an MPLS connection to each new site. 2. Connect each remote site to the customer's corporate network and route voice over the corporate WAN. |
| **Remote survivability**<br>(Basic call routing and enterprise telephony) | Available but requires the customer to purchase a SIP proxy and local gateway(s) and bring their own telephony carrier to the PureConnect Cloud data centers as well as local circuits for separate DID's. Requires customers to port their toll free circuits to their local DID's for remote survivability. |
| **Emergency dialing** | Available via customer purchased local FXO gateways (requires customer provided POTS line). Requires a PureConnect Cloud waiver with or without an FXO gateway. |
| **Application Connectivity** | |
| **Type** | **Requirement** |
| Desktop applications – Interaction client - .Net Edition and Interaction Center Business Manager (ICBM) | Connectivity to PureConnect Cloud must traverse the private MPLS connection. VPN connectivity is required if these applications are not run within the customers corporate network. |
| Terminal Services Remote Applications (TSRA) – Interaction Administrator, Interaction Attendant and ICBM | Connectivity to PureConnect Cloud is provided via the public internet. |
| Web applications | Connectivity to PureConnect Cloud is provided via the public internet. |

# Connectivity Requirements

Our customers are provided with their own Virtual Private Cloud (VPC) which consists of dedicated server instances, network security, private data storage, Network Operations Center (NOC) monitoring, and several other security measures. Typically connectivity to your service is accomplished via MPLS or Remote VPN Access (RVA) circuits unless RCM Internet Only model is deployed. The traffic traversing the circuit(s) will consist of application access, SIP signaling, switchover traffic and voice (MPLS only). Securing connectivity between the customer environment and PureConnect Cloud is a top priority for our customers.

## Domain Name Service (DNS) Requirements

Customers are required to accommodate DNS short names and Fully Qualified Domain Name (FQDN)'s for PureConnect Cloud applications to access the PureConnect cloud. Customers will need to add new Host A records to the default DNS zone of PureConnect Cloud users' PC and a new primary DNS zone. The customer's default zone referred to as

‘Customer.Local’ supports resolution of PureConnect Cloud server DNS short names from the PureConnect Cloud user PC. A new primary DNS zone named PureConnect Cloud.Local will need to be created on the customer’s DNS server(s). Host A records need to be created within this DNS zone to allow PureConnect Cloud applications to resolve FQDN addresses. Customers deploying managed IP phones for use with PureConnect Cloud will need to create Host A and Service Records (SRV) within the PureConnect Cloud.Local DNS zone as well. Example records for these requirements are listed below:

‘**Customer.Local**’ example (PureConnect Cloud server names and IP’s are provided by PureConnect Cloud):

- **Host A Record –** ‘Server001’ = 192.168.0.1
- **Host A Record –** ‘Server002’ =192.168.0.2

**CaaS.Local** example (PureConnect Cloud server names and IP’s are provided by PureConnect Cloud):

- **Host A Record –** ‘Server001’ = 192.168.0.1
- **Host A Record –** ‘Server002’ =192.168.0.2
- **Host A Record –** CaaSProvision = 192.168.0.1
- **Host A Record –** CaaSProvision = 192.168.0.2

SRV Records example PureConnect Cloud server names and IP’s are provided by PureConnect Cloud):

| Domain | Service | Protocol | Priority | Weight | Port Number | Host Offering Service |
|---|---|---|---|---|---|---|
| **CaaS.Local** | _sip | _udp | 0 | 0 | 5060 | Server0001.CaaS.Local |
| **CaaS.Local** | _sip | _udp | 0 | 0 | 5060 | Server0002.CaaS.Local |

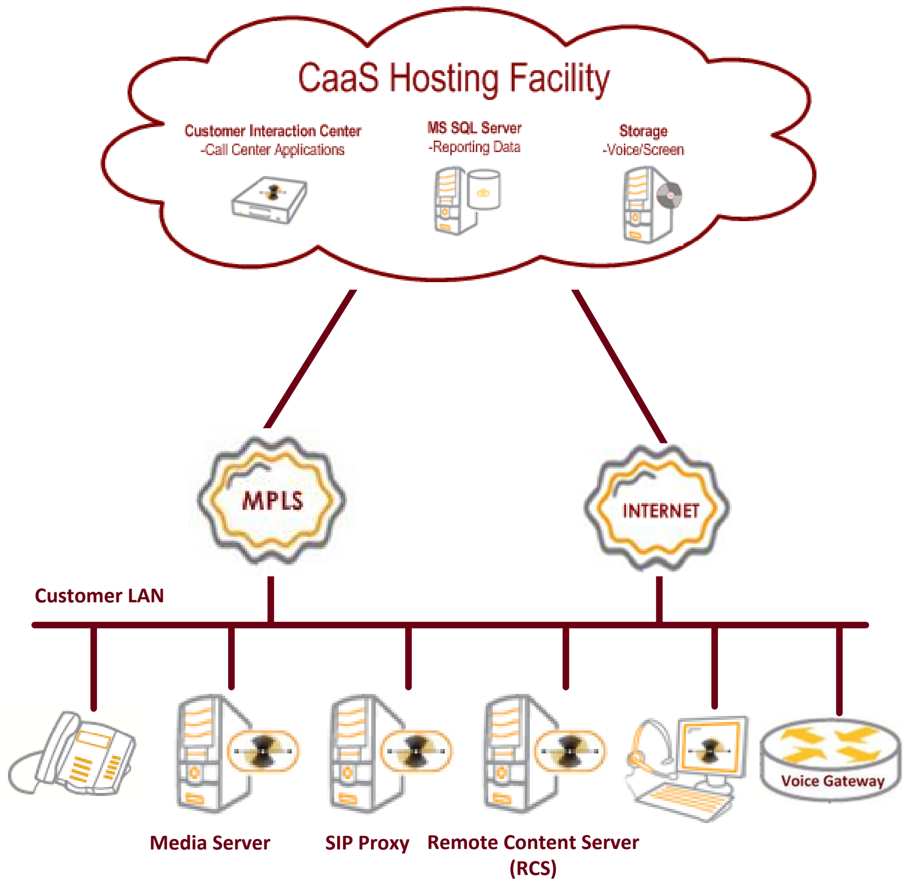
Customers are required to support DHCP Options for managed IP endpoints to function properly. The following DHCP options are required for managed IP phones:

- **Option 006 –** Name of the DNS server with the CaaS.Local DNS zone
- **Option 160 –** http://caasprovision.caas.local:8088

Additional Interaction SIP Station® DHCP option requirements:

- **Option 66 –** IP address of the primary server (example 192.168.0.1)
- **Option 67 –** Sip100.img
- **Option 132 –** VoIP VLAN ID, if the customer is using VLANs. Valid values are 0 through 4095.

# PURECONNECT CLOUD PORT REQUIREMENTS - LCM



CaaS Hosting Facility

Customer Interaction Center
-Call Center Applications

MS SQL Server
-Reporting Data

Storage
-Voice/Screen

MPLS

INTERNET

Customer LAN

Media Server

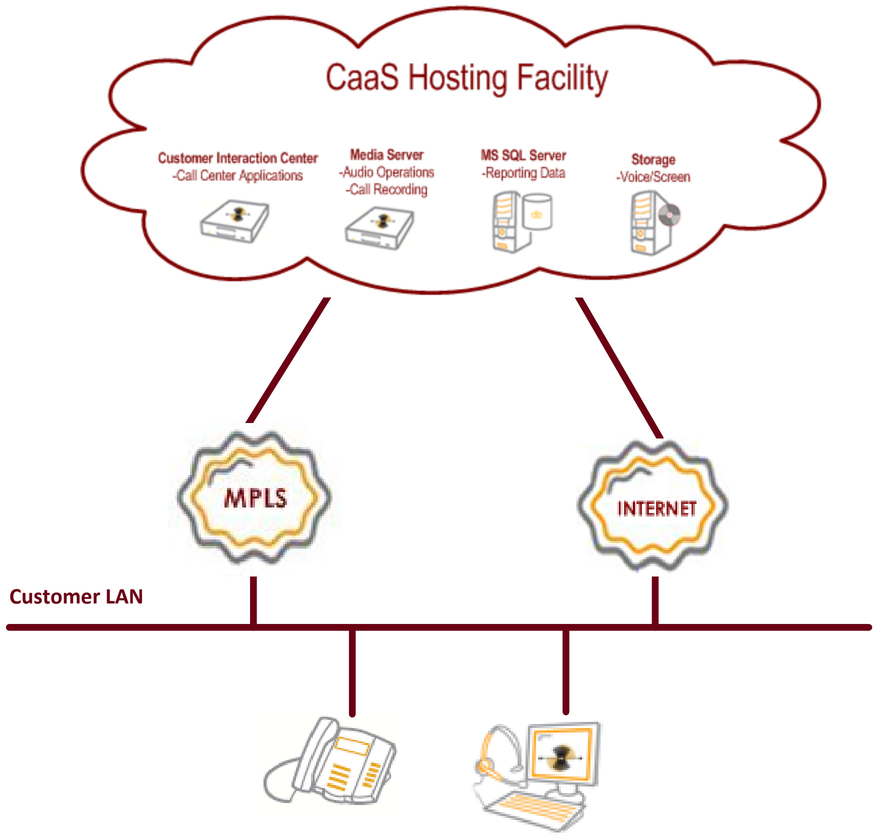
SIP Proxy

Remote Content Server (RCS)

Voice Gateway

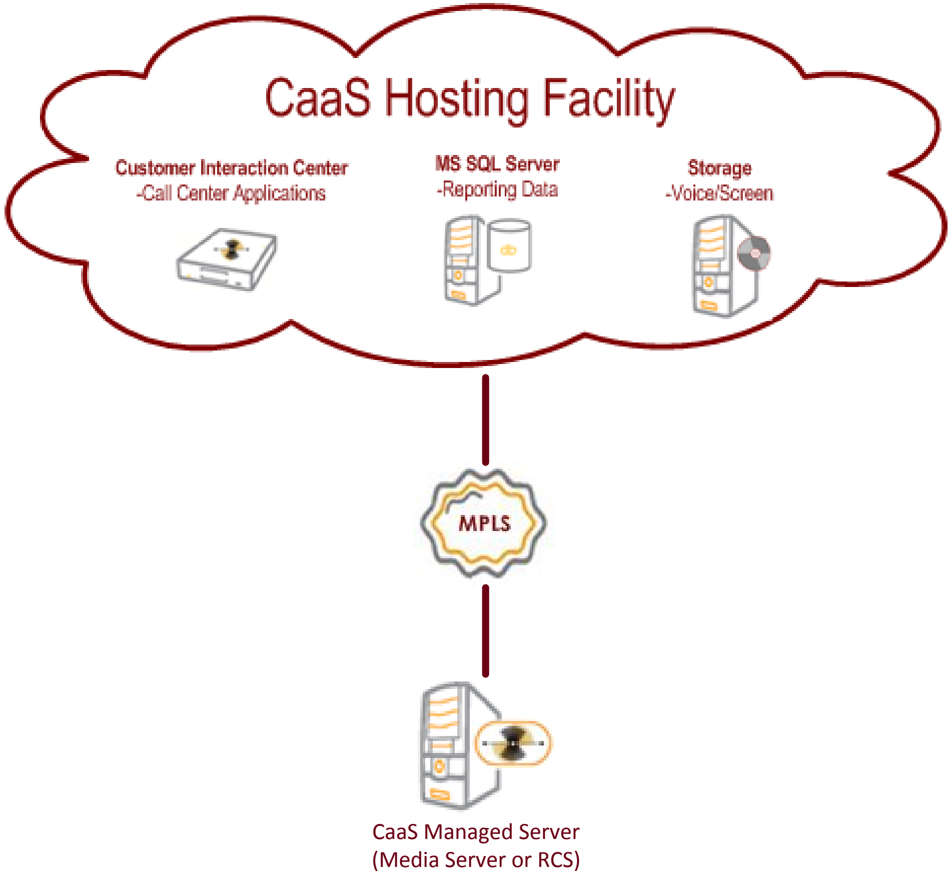
| Traffic Type | Connection Type | Protocol | Port (Range) |
|---|---|---|---|
| Web Chat | MPLS | TCP | 3508<br>8114 |
| Notifier | MPLS | TCP | 5597 |
| Notifier (RCS) | MPLS | TCP | 5597 |
| IC Management | MPLS | TCP | 2633 |
| .Net Client | MPLS | TCP | 3952<br>8018-8019 |
| Media Server | MPLS | TCP | 5004<br>5597<br>8089-8099<br>8102-8103<br>8112-8113 |
| SIP Stations | MPLS | UDP | 5060<br>8060-8061<br>8088-8089 |
| SIP Proxy | MPLS | TCP | 443<br>5060<br>8060 |
| IC Business Mgr. | MPLS | TCP | 3952<br>8106-8107 |
| TSRA | Internet | TCP | 9352 |
| Capture Client | MPLS | TCP | 8106-8107 |
| Switchover | MPLS | TCP | 2633<br>5597 |
| IMAP | MPLS | TCP | 143<br>993 |
| Microsoft EWS | MPLS | TCP | 80/443 |

# PURECONNECT CLOUD PORT REQUIREMENTS - RCM



| Traffic Type | Connection Type | Protocol | Port (Range) |
|---|---|---|---|
| RTP | MPLS | UPD | Dynamic |
| Web Chat | MPLS | TCP | 3508<br>8114 |
| Notifier (RCS) | MPLS | TCP | 5597 |
| .Net Client | MPLS | TCP | 3952<br>8018-8019 |
| SIP Stations | MPLS | UDP | 5060<br>8060<br>8088-8089 |
| IC Business Mgr. | MPLS | TCP | 8106-8107 |
| TSRA | Internet | TCP | 9352 |
| Capture Client | MPLS | TCP | 8106-8107 |
| Switchover | MPLS | TCP | 2633<br>5597 |
| IMAP | MPLS | TCP | 143<br>993 |
| Microsoft EWS | MPLS | TCP | 80/443 |

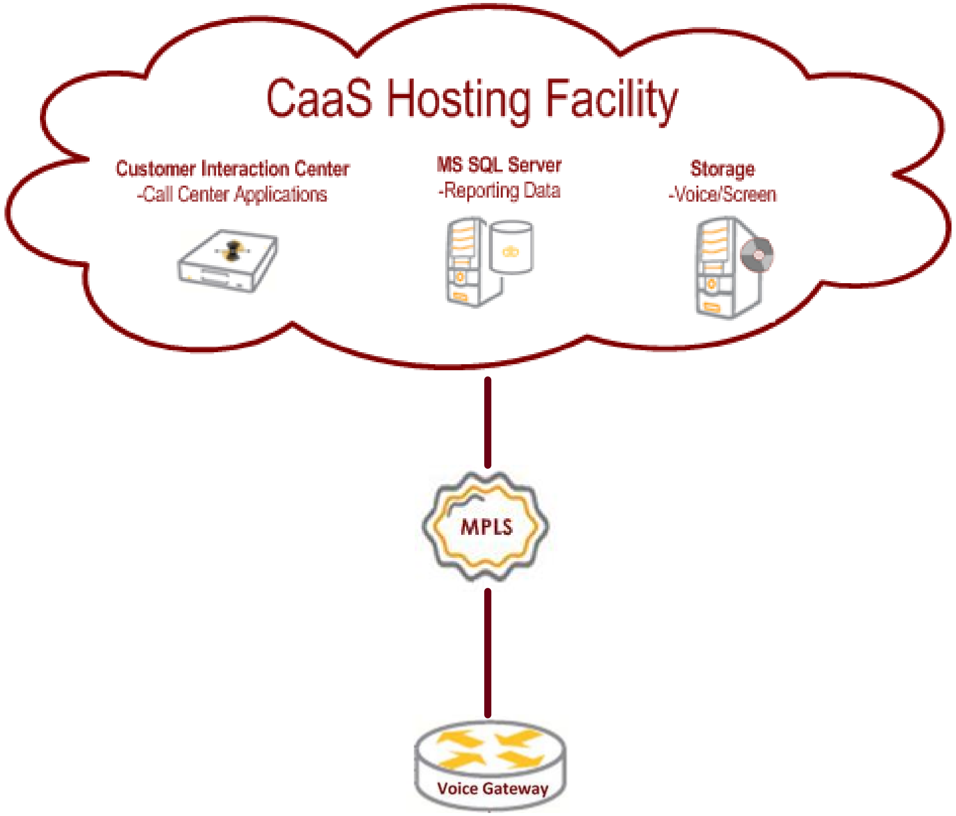
# MONITORING PORTS - APPLIANCE SERVERS



**Example: Media Servers and SIP Proxies**

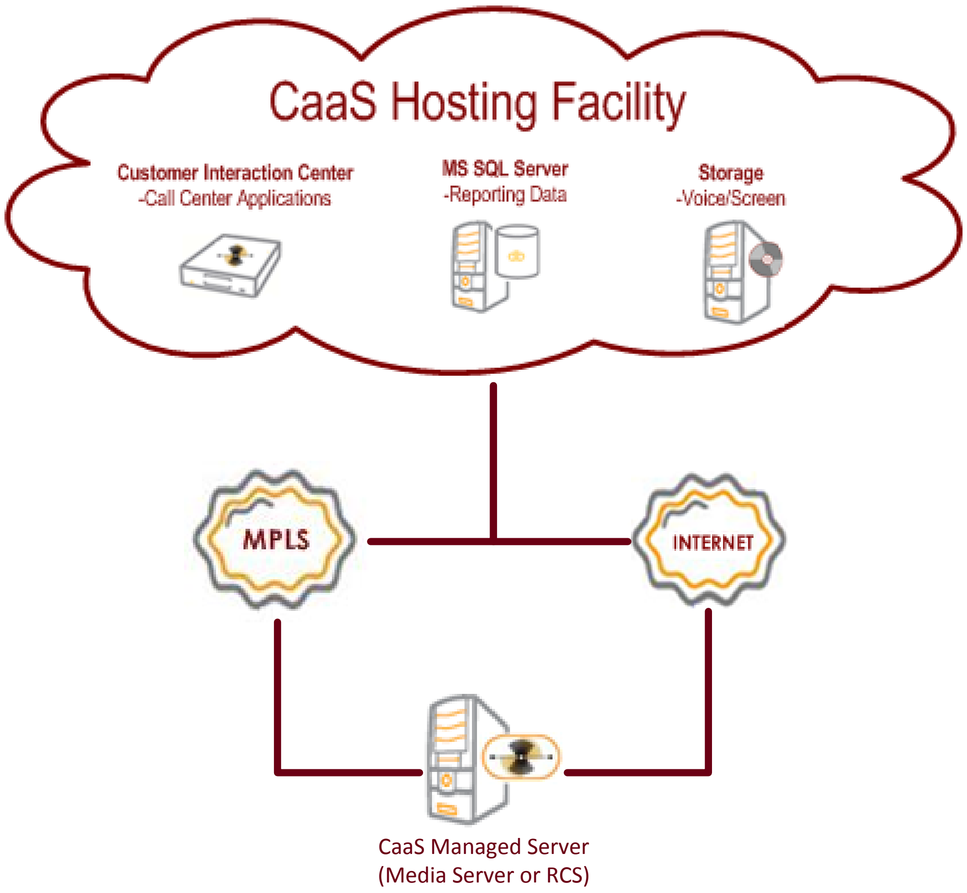
| Monitoring Tool | Protocol | Port (Range) |
|---|---|---|
| Network Monitoring Tool | TCP / UPD | 48000 – 48100 |
| Syslog | UPD | 514 |
| Remote Desktop Protocol | TCP | 3389 |
| SSH | TCP | 22 |
| HTTPS | TCP | 443 |
| iLo | TCP | 17990 |
| NTP | UDP | 123 |
| Hardware Monitoring | TCP | 2381 |
| Hardware Monitoring | TCP | 2301 |
| FTP(S) | TCP | 21<br>5004 |
| SNMP – Polling | UDP | 161 |
| SNMP – Trap | UDP | 162 |
| WMI | TCP | 5989 |
| SMB | TCP | 445 |
| MRC | TCP | 442<br>446 |

# MONITORING PORTS - APPLIANCE HARDWARE



| Voice Gateways | | |
|---|---|---|
| **Monitoring Tool** | **Protocol** | **Port (Range)** |
| Syslog | TCP / UDP | 514 |
| SSH | TCP | 22 |
| HTTPS | TCP | 443 |
| SNMP | UDP | 161 |
| SNMP – Trap | UDP | 162 |
| MRC | TCP | 442<br>444 |

# MAINTENANCE PORTS - WINDOWS AND VIRUS PROTECTION



| Type of Connection | | |
|---|---|---|
| **Update Component** | **Connection Link** | **IP Address** |
| Windows OS | Internet | PureConnect Cloud Public |
| Virus Protection | Internet | PureConnect Cloud Public |
| Release Updates | MPLS | PureConnect Cloud Private |

| Update Component | Protocol | Port (Range) |
|---|---|---|
| Windows OS | TCP | 80<br>443 |
| Virus Protection | TCP | 80<br>443 |
| Release Updates | TCP | 3389 |
| Release Updates | TCP | 445 |

## Service Deployment

Each service deployment is unique to the individual customer. The following is an example of a typical Implementation team and plan. Upon execution, of your service contract, the Service Delivery team will designate the following resources to facilitate the implementation of your new contact center solution:

- **Project Manager**
- **Implementation Engineers**
- **Application Developers (if necessary)**
- **Systems Engineers**

Service deployment consists of these major milestones:

- **Project kick-off**
- **Service base infrastructure:**
    - Virtual Private Cloud setup
    - MPLS order (if purchased from Genesys) & delivery
    - Telco order (if purchased from Genesys) & delivery
- **System configuration**
- **Functional requirements**
- **Call flows**
- **System testing**
- **User acceptance testing**
- **Training requirements**
- **Go Live:**
    - The Service Delivery team will coordinate the transition of the customer over to the Service Support team
- **Project acceptance**
- **Post go live service stabilization**
- **Service support**

Your contact center service functionality requirements ultimately drive the timeline of many of the deliverables listed above.

## Transition to Live Service

After contract signature, our Technical Account Management team will organize an initial project kick-off meeting. During this meeting your team will be introduced to your Technical Account Manager (TAM). The TAM will do an introduction, describe their role, and provide a brief overview of the future transition to normal service support. During the implementation, approximately one (1) month prior to go live services, the TAM will schedule a meeting with your team to go over the following:

- **Access to the PureConnect Support team:**
    - Create and test access accounts to the service support IVR and online case system
    - Create test support cases
    - Test access to the 'self-help' portal
- **Test NOC notifications**
- **Review support escalation procedures**
- **Confirm access to online education portal**
- **Review how to submit service requests (example: new call flow requests)**

- **Provide copy of the Service Handbook**

# Customer Administration

Genesys has developed a set of robust tools to enable you to manage your service. Each tool facilitates the management and functionality of your contact center solution. Below is a summary of each tool provided as a part of your service.

## Terminal Services Remote Access (TSRA)

Administrative applications run natively in our service cloud. Access to these applications: Interaction Attendant®, Interaction Administrator®, and Interaction Center Business Manager (ICBM), Interaction Supervisor$^{TM}$/Historical Reports are provided via Terminal Services Remote Access (TSRA). Please note, not all modules in ICBM run in TSRA, modules such as Interaction Recorder® and Interaction Dialer® run on local desktop computers. To request new user accounts, password resets, or additional access, please visit your MyCloud portal page or open a support case.

## Interaction Administrator

Interaction Administrator is the main application to facilitate the administration of: users, workgroups, phones, management of customer interaction types, and add-on features. During implementation your teams will be trained on Interaction Administrator. Access is provided without certification to your Management team. Additional courses from the Genesys Education department are available on-line and in classroom settings. Below is a list of the administration containers available to customers through Interaction Administrator:

| | | |
|---|---|---|
| | **Default Access Containers** | |
| **Account Codes** | **IP Phones** | **Stations** |
| **Actions** | **Licenses Allocation** | **Users** |
| **Client Configuration Templates** | **Password Policies** | **Workgroups** |
| **IP Phone Registration Groups** | **Roles** | **Wrap-up Categories** |
| **IP Phone Ring Sets** | **Schedules** | **Wrap-up Codes** |
| **IP Phone Templates** | **Skills** | |
| | **Available (if customer purchased)** | |
| **Interaction Analyzer** | **Interaction Feedback** | **Interaction Recorder** |
| **Interaction Dialer (includes sub containers)**<br>Base Dialer settings are restricted | **Interaction Optimizer** | **Secure Input Forms** |
| | **Interaction Process Automation** | **SIP Bridges** |
| | **Restricted By Default (available upon request)** | |
| **Client Buttons** | **Lync Status Messages** | **Station Templates** |
| **Interaction Messages** | **Queue Columns** | **Structure Parameters** |
| | **Phone Numbers**<br>Available **only** if customer brings their own carrier | **Web Service Parameters** |
| **Interaction Tracker** | **Reports** | **SMS Broker** |
| **IP Tables** | **Response Management** | **SMS Configuration** |
| **Mail Configuration** | **Station Groups** | **Licenses Allocation** |
| **Lync Configuration** | **Station Messages** | **Single Sign-On** |

## Interaction Attendant

Interaction Attendant is an application that allows your team to create simple or sophisticated auto attendant voice and IVR applications. Interaction Email Attendant provides similar functionality for email queuing. Customers are provided with full access to this administrative tool. On top of the training received during service deployment, it is highly recommended individuals complete one of the following: an instructor led web-based or a classroom based course provided by Genesys' Education department on Interaction Attendant.

A support case is required to be opened in order to have audio prompts added for use with your service.

## Interaction Center Business Manager (ICBM)

ICBM is an application that consists of management modules for: Interaction Recorder, Interaction Supervisor, Interaction Dialer, and Interaction Reporter. Your team will be trained on ICBM as a part of your service deployment. Full access will be granted to these modules without certification or prerequisite training. On-line and classroom educational courses are available should additional training be desired.

## Interaction Designer

Interaction Designer is a GUI desktop application used to create, modify, and manage handlers. Interaction Designer is available to all editions to customers who have completed Interaction Handler Certification. Access to Interaction Designer is limited to non-production environments only.

# Service Support

Our Support team provides complete assistance on issues ranging from 'how to' types of questions to software defect issues. We provide you with the tools, information, and assistance necessary to run your contact center efficiently and effectively.

Our Support team members are located globally to provide coverage around the clock. For a list of global offices, please refer to the following link: http://www.genesys.com/about/contact-us/global-offices

## Contacting Support

Only designated contacts are provided access to our support sites and staff. Designated contacts are provided with an IVR pin code and a username/password for our online issue tracking system. Please note you can use your IVR passcode for phone support if we do not have your phone number stored in our systems. This IVR passcode can always be found on our online issue tracking system: https://genesyspartner.force.com/customercare/ under Manage Profile -> My Profile -> IVR Code/Pin. Please visit the 'Contact Us' page for more information on how to contact us: https://genesyspartner.force.com/customercare/CustomerCareContactUs.

## Access to Support

PureConnect Support is available 24 hours a day, 7 days a week, for all support inquires and case priorities. We'll be there when you need us, regardless of case priority. This is done by leveraging our global, follow-the-sun presence to provide support to you.

Follow-the-sun presence means you may not always receive support from someone in your geographic region, however it does mean you'll reach the best skilled engineer to address your case.

Please note that our support services for Latin America, Brazil, and Japan will continue to follow established normal business hours to leverage local language expertise.

## Contacting Technical Support

For your convenience, we offer the ability to report your cases via the My Support Portal. This is the preferred method of case submission. For these, you will receive a call back from one of our skilled engineers. You can also submit a new case via the phone by utilizing our IVR. Please keep in mind that we will be fielding live phone calls first.

For our global IVR phone numbers and a link to our online case tracking system, please see our Contact page at https://genesyspartner.force.com/customercare/CustomerCareContactUs. Please note that you will always need your PIN code. This PIN code can be obtained by logging into My Support Portal -> Manage Profile -> My Profile.

If you do not have access to the online case tracking system, you will need to e-mail support.customercare@genesys.com.

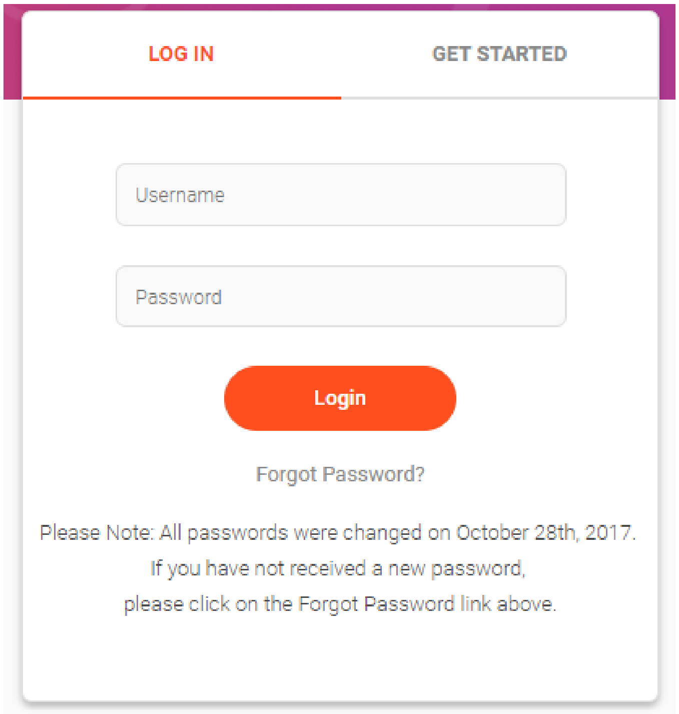
In the event of an after-hours emergency, please contact PureConnect Support via phone. You should indicate in the IVR that this is an emergency.

We ask you not to e-mail or call an individual because at any time an individual may be out of the office or away from their desk for an extended period of time. Please call in through our IVR and use the appropriate routing to be connected to an agent.

## Opening a new web Case

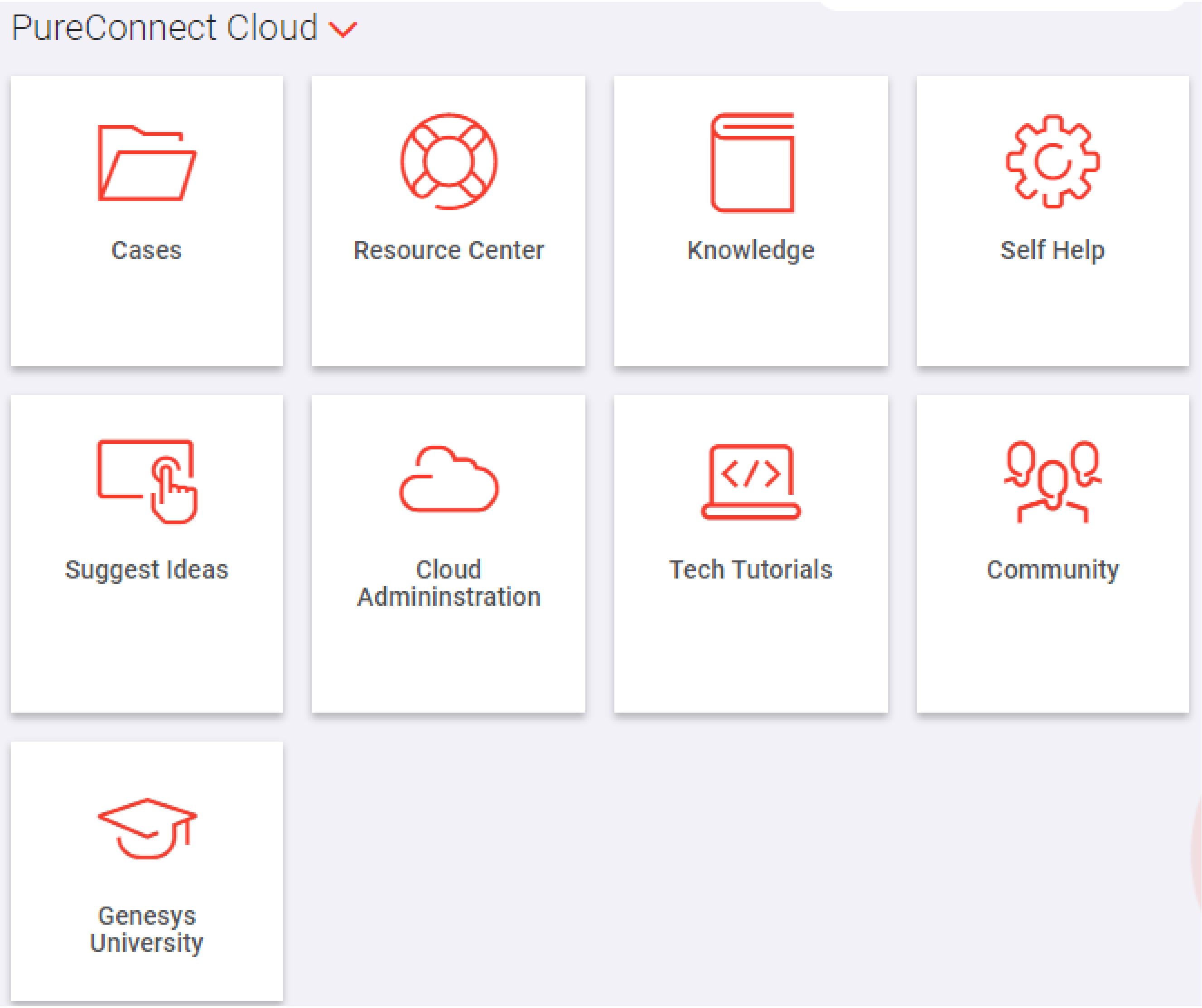
Navigate to https://genesyspartner.force.com/customercare/

- Log on to the following screen using the credentials that have been emailed to you.

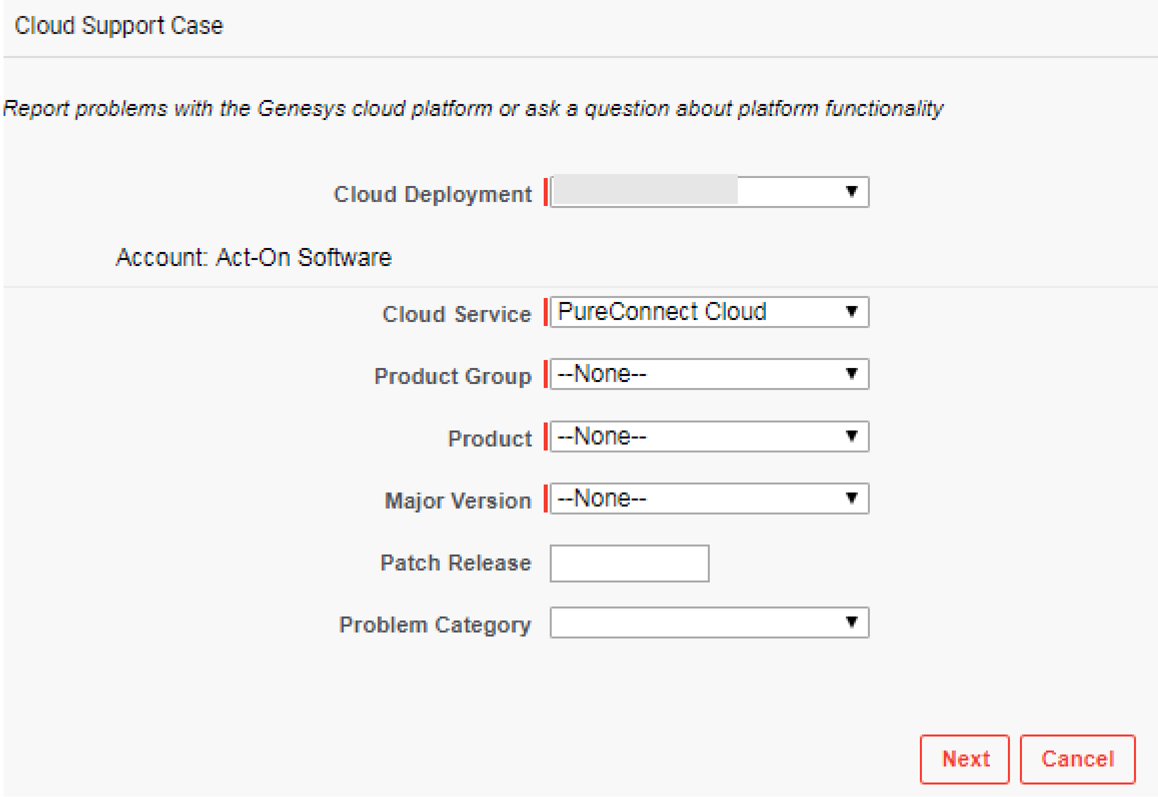


Please Note: All passwords were changed on October 28th, 2017.
If you have not received a new password,
please click on the Forgot Password link above.

- Once logged in, you should see this screen



- To open a new incident, under ***Cases***, select the Open a Support Case or Open a Service Request for a MAC case
- Fill in the appropriate product group and product that the issue is in as well as major version



Cloud Support Case

*Report problems with the Genesys cloud platform or ask a question about platform functionality*

Cloud Deployment ▼

Account: Act-On Software

Cloud Service: PureConnect Cloud ▼

Product Group: --None-- ▼

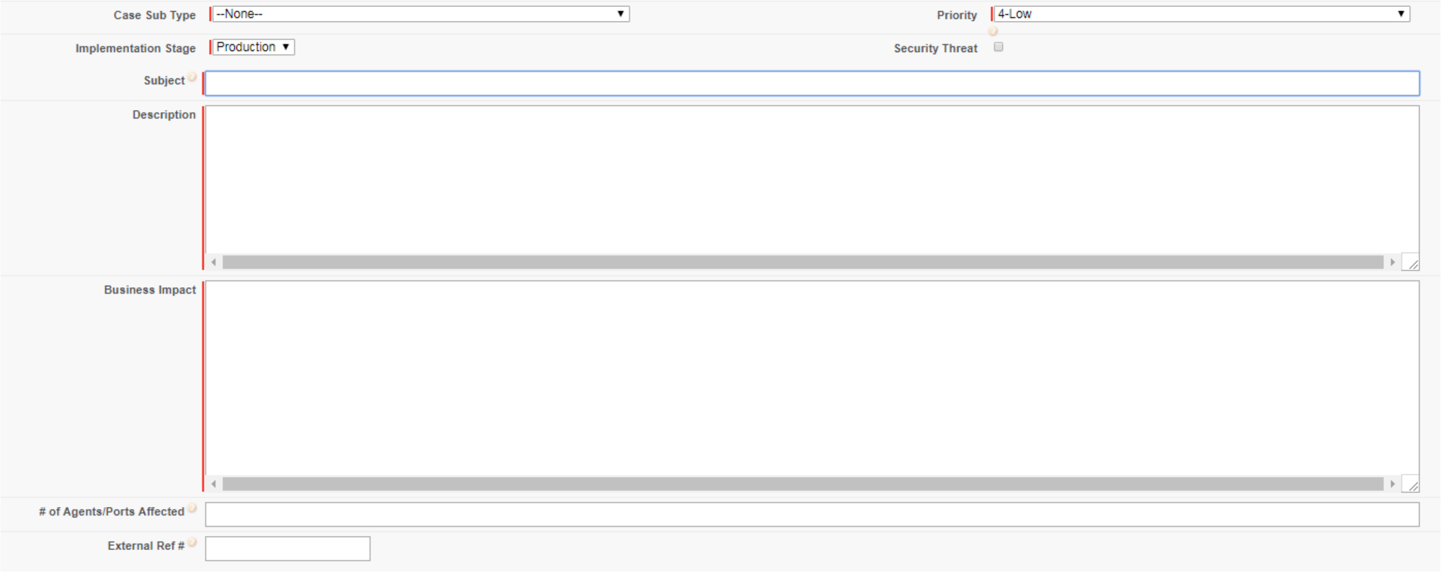
Product: --None-- ▼

Major Version: --None-- ▼

Patch Release:

Problem Category: ▼

- Fill in the required information for the issue you are experiencing.
  - Case sub type: Problem or Inquiry
  - Environment Type: What environment the issue exists in (dev or prod)
  - Priority: Choose priority of case.  Automatically defaults to low
  - Subject: Brief description of problem
  - Description of Issue: Be as descriptive as possible including if there were any recent changes
  - Business Impact: i.e. number of agents/calls affected



Case Sub Type: --None-- ▼

Priority: 4-Low ▼

Implementation Stage: Production ▼

Security Threat: □

Subject:

Description:

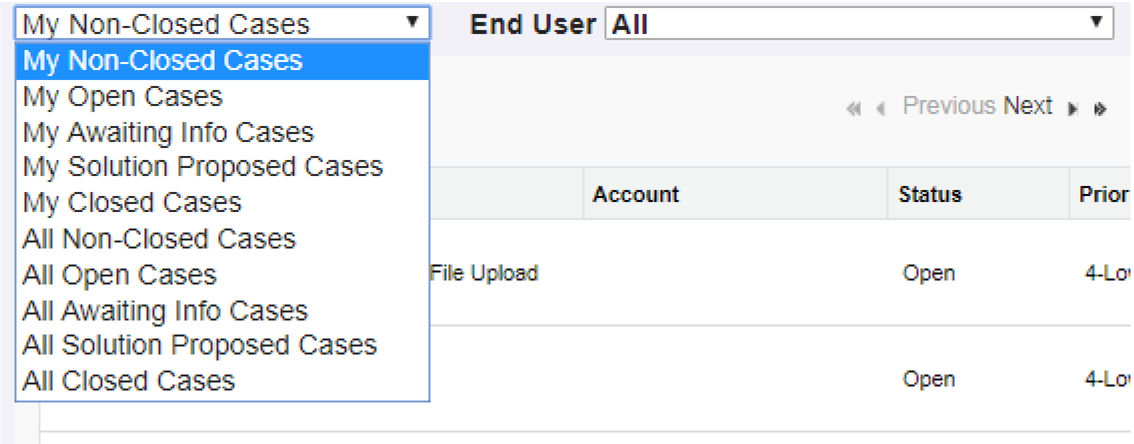
Business Impact:

# of Agents/Ports Affected:

External Ref #:

# Viewing/Managing Cases

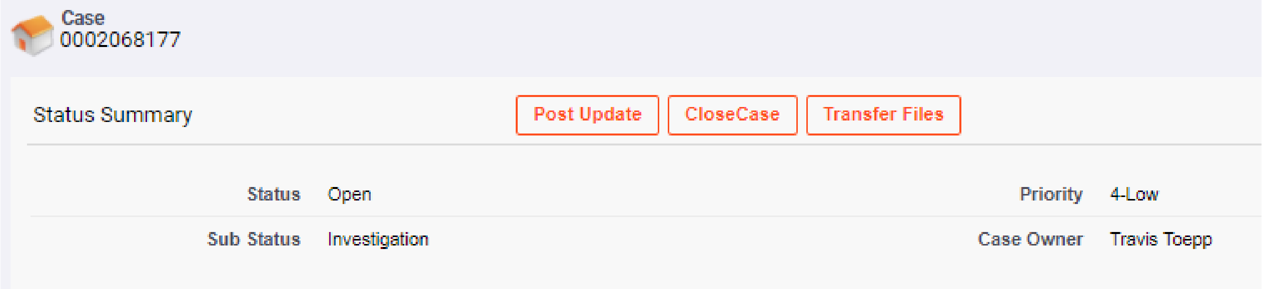
- Navigate to https://genesyspartner.force.com/customercare/
- Log on to the My Support Portal using the credentials that have been emailed to you.
- Navigate to Cases -> View/Manage Cases. Choose which case view you want to use.
  - Note: If you need the ability to see your colleagues' cases, please request permission to do so by opening an Admin case or emailing customercare@genesys.com. You can then view by going to All Open cases as shown below.



End User All

| | Account | Status | Prior |
|---|---|---|---|
| File Upload | | Open | 4-Lo |
| | | Open | 4-Lo |

- From here you can choose the specific case you want to update/view
- Once in a case, you can choose to update, close, or upload files



Case
0002068177

Status Summary

| | | | |
|---|---|---|---|
| Status | Open | Priority | 4-Low |
| Sub Status | Investigation | Case Owner | Travis Toepp |

## Transfer Files to/from Case

Genesys provides a file transfer tool on My Support to allow customers to upload logs and other files that may be needed to help resolve Cases. Clicking the Transfer Files button within any non-closed Case launches the browser-based File Transfer Client, which provides the following features:

- Secured data transfer over HTTPS
- Sending multiple files concurrently
- File transfer resume capability
- Integrity validation
- No file size limit

### Browser Settings and Other System Requirements

To use the built-in file transfer tool, the following settings must be in place:
The browser running the client must have cookies enabled.
The browser must allow pop-ups from the following servers for the Transfer Files functionality to work properly.
https://eftgateway-us.genesys.com

https://eftgateway-emea.genesys.com
https://eftgateway-apac.genesys.com

The following browser versions are currently supported:

- Internet Explorer v11 or later
- Chrome v44 or later
- Firefox v39 or later
- Safari v8 or later on Mac OS

### Temporary FTP Accounts

A situation may arise when the file transfer tool on My Support cannot be used for a given transaction. To address this need, Genesys has established the Temporary FTP Account process.

For a given Case, you can ask Customer Care to create a temporary FTP account, and then use an SFTP client application of your choice to transfer the files. Potential SFTP clients for Windows users include WinSCP, FileZilla, CuteFTP, PSFTP, Core FTP, and Fire FTP. Potential SFTP clients for Mac OS users include FileZilla, ClassicFTP, Fire FTP, Secure FTP, and Cross FTP. Unix users can use the SFTP utilities built into the operating system.

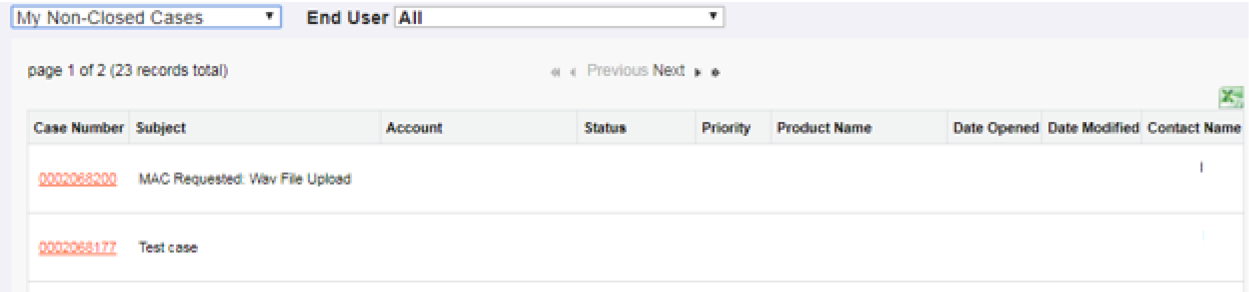
Once the temporary account is created, it will be associated with the given Case and remain active for the next 5 days (120 hours total). The login credentials along with the expiration date will be displayed in the Temporary FTP Account section of the Case details page while the temporary account is active.

## Update an Open Case

There are 2 ways to update a case: via My Support portal or via Email

### Update via My Support Portal:

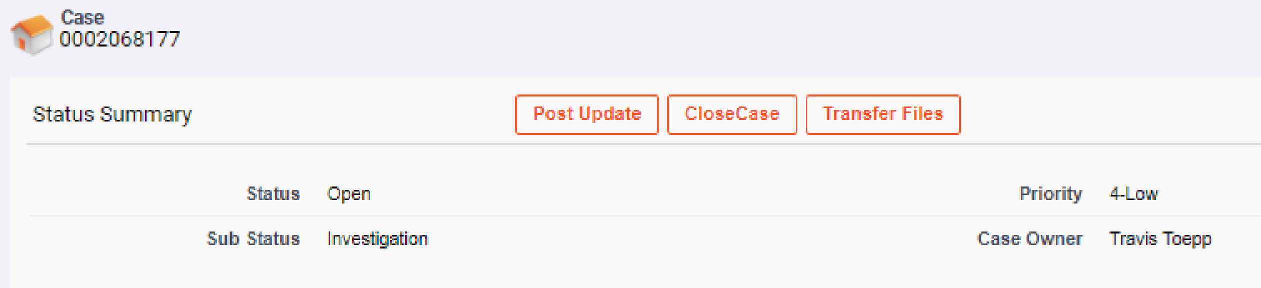
- Click the Case number you want to update



page 1 of 2 (23 records total)

| Case Number | Subject | Account | Status | Priority | Product Name | Date Opened | Date Modified | Contact Name |
|---|---|---|---|---|---|---|---|---|
| 0002068200 | MAC Requested: Wav File Upload | | | | | | | |
| 0002068177 | Test case | | | | | | | |

- Click ‘Post Update’ in the top bar
  - Note: The portal update does not support rich text. Please use the email response back to the case if you need rich text for your update.

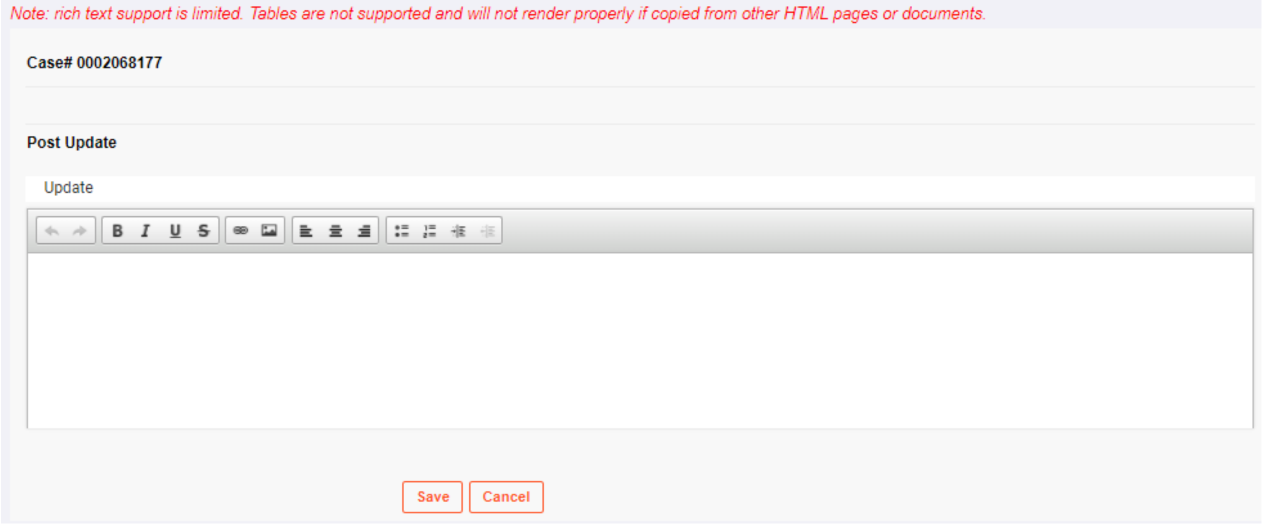


Case
0002068177

Status Summary

Status Open
Priority 4-Low
Sub Status Investigation
Case Owner Travis Toepp

- A separate window opens for you to add your update.  Once finished, click Save at bottom of page


Note: rich text support is limited. Tables are not supported and will not render properly if copied from other HTML pages or documents.

Case# 0002068177

Post Update

Update

## Update via Email

You can update an Open Case by Email if you reply to an Email originated from the Case by a Genesys Customer Care representative or to an automated Case notification. An Email originated from a Case includes a special Reference ID, which ties any reply back to the Case.
On the contrary, if you start a new Email and send it to Customer Care , it will not link to the Case automatically, even if you have specified a Case #. Such an Email will be processed by the Customer Care Admin team and may be manually linked to the Case specified, but automatic linkage will not occur unless the Email body contains the Reference ID.

NOTE: If the Case is in Awaiting Info or Solution Proposed status, and the Case contact replies to an Email originated from the Case, this will also change the Case Status to Open. In addition to this, will also see the Email updates in the Case Updates section of the Case.

## Auto Follow-Up Process

The Automated Follow-up Service is designed to ensure timely and proactive follow-up with customers when we need information to advance a Case towards resolution. Automated Follow-ups will be sent to the Customer Contact on the Case according to the rules outlined below.

**Auto Follow-Up #1**: When Customer Care proposes a solution or requests information for an open Case, a follow-up timer is started for that Case. If there is no customer response within two (2) business days, an automated Email is sent to the customer contact who opened the Case, with a reminder of the customer action requested (provide information or accept/reject solution), and a link to access the Case.

**Auto Follow-Up #2**: If there is no customer response within five (5) business days after Customer Care proposes a solution or requests information for a Case, a second automated Email is sent to the customer contact who opened the Case. This email contains a reminder of the customer action requested (provide information or accept/reject solution), and a link to access the Case.

**Auto Follow-Up #3**: If there is no customer response within ten (10) business days after Customer Care proposes a solution or requests information for a Case, the Case is closed and a final auto follow-up Email is sent to the Customer

Contact who opened the Case. All information in the Case will remain intact for one month (including any logs or attachments). The customer can reopen it only by a telephone call to Customer Care.

***NOTE:***

- This automated follow-up process applies to all Cases with Critical, High, Medium or Low priority.
- Automated follow-ups are not used for Critical - Production Down cases.
- The follow-up timer could start and stop several times for a given case. Some examples of requests that start the follow-up timer:
    - Send environment information
    - Describe what happened before application failure
    - Send product logs
    - Verify proposed solution

## Closing Cases

You can close a Case through **My Support** using the following steps:

1. Login to **My Support** using the corporate email listed in your user profile.
2. Go to your dashboard, Select **Cases** and then **View and Manage Cases**.
3. Select the Case you want to close.
4. Click the Close Case button.
5. Select either Resolved or Cancelled as the Sub Status.
6. Enter your Closure Comment.
7. Select Close Case.

Genesys Customer Care will close a Case for the following reasons:

- The proposed solution or answer provided by Customer Care has been accepted by the Customer.
- The Customer requests closure/cancellation of the Case.
- Genesys has sent three automated follow-ups about the Case without a response from the Customer. For more information, see the Auto Follow-Up Process in the Managing Cases section.

All attached data in a closed Case (including any logs or other customer files) is purged from **My Support** one month after the case is closed.

If you reopen a Case more than 30 days after it was closed, you will need to resubmit the attached data since it is purged 30 days after the Case is closed.

## Reopening Cases

A previously closed Case may be reopened if an issue has not been resolved or if a Case was closed by accident.
For the Case to be reopened, all new supporting information demonstrating that an issue has not been resolved should be supplied to Genesys Customer Care within ***30 days*** from Case closure. Without this information, the Case will not be reopened. The Customer can reopen a Case by:

- Login to **My Support**, go to your dashboard and select **View and Manage Cases** located behind the **Cases** , view My Closed Cases or All Closed Cases, then select the case and click "Request to Re-open" at the top.

***Note: This function will only be available for Cases closed within 30 days from Case closure.***

- Call Customer Care.

For Cases closed more than 30 days, contact Customer Care or create a new Case so supporting information can be supplied.

# Contacting Technical Support Management

If you have a case that requires management assistance, please first ensure that a support case has been logged for use as a point of reference. In addition, be sure to indicate the priority/impact in the support case. We cannot address the escalation until it has been properly reported to our technical support team.

Please use the following as guiding criteria to consider prior to requesting escalation of an existing case.  Note that if an escalation requires engagement of development, cloud operations, or a 3rd party, please understand that it may require additional time to resolve pending their analysis and findings.

- An escalation should not be requested due to a request for RCA unless we've had 5 business days for cloud deployments to complete analysis per our standard Service Level Targets for RCA delivery.
- Please do not escalate based on change in urgency/impact. Please request change of priority of case per the recommendation below.
    - If case needs to be changed to a high priority based on a greater need for urgency or broader impact, please call in the request to our care team.
- If a high priority case has not been updated in the last 24 hours and the case is actively causing significant business impact, an escalation can be requested.
- If a medium case has not been updated for 3 business days, it is eligible for escalation if required. If impact of the issue has changed to a higher priority, please contact our care team to request a change in priority based on urgency/impact
- Low priority cases are not eligible for escalation, if the impact of a low priority case changes, please request a change to medium through a work note in the case. If a change to high is required, please contact our care team by phone.

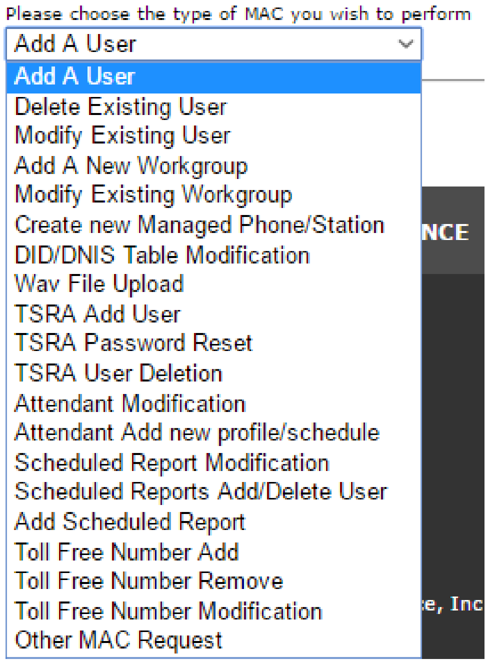
If you have a case that requires management assistance, please send an email to PureConnectCCManagementAttention@genesys.com with the following information:

Subject: Customer Name - Case No. - Description
Case No.:
Escalation Reason (Impact/Urgency):
Product:
Version Major/Patch:
Summary:
Critical dates/times such as go lives, follow up internal meetings
Expectations

# Types of Cases

## Service Request Cases

These are for Move, Add, and Changes (MAC) cases.  MACs are PureConnect system changes typically made to individual users only, but not in all cases.  These are the most common types of changes made on customer systems. Below is a list of Move, Add, and Changes (MAC) that are covered


Please choose the type of MAC you wish to perform
Add A User
Add A User
Delete Existing User
Modify Existing User
Add A New Workgroup
Modify Existing Workgroup
Create new Managed Phone/Station
DID/DNIS Table Modification
Wav File Upload
TSRA Add User
TSRA Password Reset
TSRA User Deletion
Attendant Modification
Attendant Add new profile/schedule
Scheduled Report Modification
Scheduled Reports Add/Delete User
Add Scheduled Report
Toll Free Number Add
Toll Free Number Remove
Toll Free Number Modification
Other MAC Request
NCE
e, Inc

In most cases, a Web form is available.  Web forms ensure that all required information necessary for the change request is provided.  Additional Web forms will be created as needed.  All other changes will be handled on Time & Material (T&M) contract basis.

## Support Cases

A trouble Case should be opened for any unexplained behavior of the PureConnect platform.  Support Cases can be opened via the web portal and via the phone.  For the timeliest results, it is recommended that cases be opened via the phone.

## Admin Cases

These cases are used for problems or questions related to your My Support Portal account.  These are usually access
Open an Admin Case for the following reasons:

- Obtaining support access to a particular service contract or Sold To/End User account combination
- **My Support** changes such as adding or removing a contact or updating an email address
- Requesting **My Support** access level changes
- Changes with your Genesys account
- Problems with your licenses
- **My Support** functionality issues
- Product does not show in drop-down list
- File upload/download issues when using "File Transfer" function
- Requesting Log File Retrieval Service

To submit an Admin Case:

1. Select **Open Admin Case** located after selecting **Manage Profile** from the header.
2. Populate each Mandatory Field with the required information.
3. Click Submit.

To check the status and manage your Admin Cases:

1. Select Manage Admin Case from the left-side menu

## Monthly Customer Reports

On a monthly basis, we will provide your Management team with a case summary report that details support and Service Level Agreement (SLA) uptime. Reports are delivered within the first five (5) days of each new month. Service impacting cases that were closed within the reporting period will specify downtime, if applicable. In order to receive this report, a request can be made to your Technical Account Manager. Please specify the email address to which you wish to have the report delivered.

## Self Help Resources

Your team will have access to Genesys' product support portal (https://genesyspartner.force.com/customercare/). Detailed product and feature documentation can be found, along with useful troubleshooting tips. Below are some of the most helpful sections:

- **Resource Center** – The resource center section organizes official release information, documentation, system prerequisites, updates, and recommendations for each PureConnect product and their respective telephony platforms. Expect to find installation guides, software downloads, and supported configurations.
- **Self Help –** This section is maintained by Genesys' Support team and provides more in-depth troubleshooting information categorized by topic or component. Each section will provide insight to common problems and solutions, and the information to collect to troubleshoot other issues.
- **Cases** – You will be able to view your open support cases, open MAC cases, search previous cases, search past ISupport cases, or open new cases via the web.
- **Cloud Administration –** MyCloud is a web-based portal for customers to administer and view details of the PureConnect Cloud solution. MyCloud offers an intuitive user interface that allows you to manage various aspects of your solution. MyCloud offers you the following capabilities:
    - MyCloud user management
    - Terminal Services Remote Access (TSRA) user management:
        - TSRA password reset
        - TSRA user creation
        - TSRA user enable/disable
    - License usage tracking history:
        - Billing reports
        - User detail reports
    - Media file management:
        - Custom handlers
        - Music on hold (.wav files)
        - Audio prompts (.wav files)
        - Grammar files

The MyCloud portal may be accessed via http://mycloud.inin.com/login. To delete MyCloud users, please email issues@genesys.com.

## PureConnect Cloud Provided Support Tools

Your certified staff members will be provided with the following tools via MyCloud for the expressed purpose of Level 1 troubleshooting:

- **Interaction Center Log Viewer**
  - Access to all xIC logs on all PureConnect systems delivering service (includes Development systems)
- **Future Tools via MyCloud or Direct Access**
  - Windows Event Viewer:
    - System Logs
    - App Event Logs
  - DSEditU or RegEdit (Read Only)

## Carrier Support

Support for carrier services, such as MPLS and / or Telco, is provided by our Support team when these services are purchased directly from Genesys. The Support team will interface with our carrier, on your behalf, to provide support continuity for all components used in service delivery. Normal case processes and procedures apply. If carrier services are not purchased through Genesys, carrier engagement is the customer's responsibility.

## Moves, Adds and Changes (MAC)

MACs are classified as minor administrative additions, changes, and deletions to your contact center service. MACs are billed at your contract rate. Multiple requests may be grouped into a single MAC case request; however, the cumulative time to complete the MAC request cannot exceed one (1) hour of work. All change requests are subject to approval via our change control policy. Typical MAC requests are listed below:

| **Example: Additions, changes and deletions** | |
|---|---|
| Users<br>Stations / Managed Phones<br>Client Templates<br>Workgroups<br>Roles<br>Status Messages<br>Dial Plan | Password Policies<br>System Schedules<br>Schedule Reports<br>Account / Wrap-up Codes<br>ACD Skills<br>Interaction Recorder – policies and rules<br>Interaction Dialer –campaign creation |

** MAC requests are subject to your Service Level Agreement (SLA)*

## Release Upgrades

Release updates are covered under maintenance for your service and are considered to be non-billable work. The following services are provided as part of the release upgrade process:

### Project Management

A member of the PureConnect Cloud Services team will be identified to provide project management to the customer and prepare the following:

- **Project plan:**
  - A project plan based around the devices to be upgraded.

  - The project plan will be an overall schedule based on the amount of time anticipated for device upgrade.

## Pre-Implementation

- Schedule kick-off call to discuss goals of upgrade (i.e. customer request or Genesys requirement).
- Information regarding the changes that have been made in the release update will be provided, as required by the customer.
  - Customer is responsible for reviewing these changes to make sure that their business processes are not impacted (see testing).
- PureConnect Cloud Services can provide correlation between cases closed due to SCR and SCR release update inclusion.

## Client Application Upgrades

- Installation files for the Interaction Center (IC) Client upgrade will be provided to the customer prior to the start of the IC server upgrade.
- New files for the remote applications (Interaction Attendant®, Interaction Administrator® and Interaction Supervisor™) will be provided prior to the start of the IC server upgrade.
- Client application upgrades are customer driven; however, if there is a client related issue reported while a user is using an old version of the client, Support will request they upgrade to the latest version.

## Implementation

- A member from the PureConnect Cloud Implementation team will be identified to assist with the upgrade of the PureConnect environment.
- Devices will be upgraded as indicated on the device upgrade list.
- The Implementation team is responsible for all server software installation and configuration as required by the upgrade.

## Testing

- The PureConnect Cloud Services team will provide a standard Basic Functionality Test (BFT) plan. Following the upgrade, the BFT will be executed by the customer.
- The customer is responsible for providing and creating their own User Acceptance Test (UAT) plan or they can refer to their test plans that were used at the time of implementation.

## Support

- A member of the PureConnect Cloud Services team will provide support throughout the testing process to ensure that the upgrade has been completed successfully.
- PureConnect Cloud Services will work with PureConnect Support should there be any issues.
- Once the upgrade has been agreed upon as being successful, the customer should resume standard support methods.

# Customer Responsibilities

Getting the most out of our contact center solution is a top priority for Genesys. As a customer of our service, your responsibilities include, but are not limited to: support case management, support of our operational teams for service maintenance, physical and logical access to systems we manage, and support of your internal network.

- **Designated Contacts –** Must have at least two (2) designated contacts to access Genesys support, or a partner must engage support on your behalf.
  - **Transitioning to Genesys Support** – Should you transfer from Partner provided support to direct Genesys Support you will be required to have two (2) designated contacts.

    - **Partner Provided Support** – If you purchase support from a Partner, this certification requirement does not apply.
- **Support Case Management –** Certified individuals to access the Support team
    - **Case Ownership –** Your team's case owners or partner are required to work cooperatively with our Support staff.
    - **Management Oversight –** If reported support cases span multiple groups within your organization, coordination, and prioritization may be required from your team.
- **Operations Support–** Patches and updates will be applied periodically as a part of the service. A designated point of contact from your organization is required for maintenance window approval and coordination of service upgrades.
- **Access:**
    - **Customer Supplied Applications –** Any applications, supplied by your organization, such as Microsoft SQL are the responsibility of the customer for management, maintenance, and administration unless otherwise specified.
    - **Systems Access –** For any system or server managed by our Service Operation teams a local account is required to be supplied for service operation.
    - **Physical –** For any device managed by Genesys as a part of our service physical access must be provided upon request.
- **Network Support –** In the event of connectivity problems between our data centers, and your service locations, support from your Network team will be required.
- **Internal Change Control –** Access to the administrative applications of your service are provided to certified staff members. Implementation of change control, for any changes your staff implements, in applications such as Interaction Attendant and Interaction Administrator is required.

## Required Information for Support Cases

To assist in rapid closure of cases, please be prepared to provide the following information to our Support team during the troubleshooting process:

1. Provide a detailed description of the incident.
2. When is the issue occurring? When is the issue not occurring?
3. A timeline of when the reported incident started to happen and did this ever work?
4. Does the issue affect all users? If not, what is the profile and pattern of the users affected?
5. Does the issue affect all of the lines or calls? If not, what is the profile and pattern of the calls that are affected or incident that is being reported?
6. What recent changes have been made? When were these changes made?
7. If applicable, provide individual call IDs for the reported examples.
8. Is the problem reproducible? If so, what are the steps to reproduce the issue?

For web cases, please provide this information in the case at time of submission.

## Responsibility Assignment Matrix

The chart below provides a high level overview of the tasks required to deliver your contact solution service. Any items not specifically referenced below will be considered your team's responsibility.

| Responsibility Assignment Matrix | | | |
| --- | --- | --- | --- |
| **Responsibility / Task** | **Genesys** | | **Customer** |
| | **LCM** | **RCM** | |
| ***Version Upgrades*** | | | |
| *Project Management* | ✓ | ✓ | |
| *Application Upgrades* | ✓ | ✓ | |
| *Networking Updates* | ✓ | ✓ | ✓ |
| *Client Installation* | | | ✓ |
| *System Testing* | ✓ | ✓ | |
| *User Acceptance Testing (UAT)* | | | ✓ |
| ***Release Updates*** | | | |
| *Project Management* | ✓ | ✓ | |
| *Application Upgrades* | ✓ | ✓ | |
| *System Testing* | ✓ | ✓ | |
| *Updated Client Installation* | | | ✓ |
| *User Acceptance Testing (UAT)* | | | ✓ |
| ***Service Delivery Infrastructure*** | | | |
| *Gateway Upgrades (Customer-controlled)* | | | ✓ |
| *Server OS & Antivirus Patches (Genesys-controlled)* | ✓ | ✓ | |
| *Server OS & Antivirus Patches (Customer-controlled)* | | | ✓ |
| *Networking Maintenance* | ✓ | ✓ | ✓ |
| *Cloud Storage Maintenance (Genesys-controlled)* | ✓ | ✓ | |
| *Storage Maintenance (Customer-controlled)* | | | ✓ |
| *SQL Maintenance (Genesys-controlled)* | ✓ | ✓ | |
| *SQL Maintenance (Customer-controlled)* | | | ✓ |
| ***Telco & MPLS Services*** | | | |
| *PureConnect Cloud Provided* | ✓ | ✓ | |
| *Customer Provided* | | | ✓ |
| ***Security*** | | | |
| *Certifications and Audits* | ✓ | ✓ | |
| *Change Control* | ✓ | ✓ | ✓ |
| ***Monitoring & Alerting (24/7/365)*** | | | |
| *Application Servers (Genesys-controlled)* | ✓ | ✓ | |
| *Application Servers (Customer-controlled)* | | | ✓ |
| *Core Infrastructure* | ✓ | ✓ | |
| ***Support*** | | | |
| *Service Feature Support* | ✓ | ✓ | |
| *Third-Party Integrations (Genesys Provided)* | ✓ | ✓ | |
| *Third-Party Integrations (Vendor/Service Management)* | | | ✓ |
| *Local Site Support* | | | ✓ |
| *Local Workstation Logs* | | | ✓ |
| *Packet Captures (PureConnect Cloud Network)* | ✓ | ✓ | |
| *Packet Captures (Customer Network)* | | | ✓ |

# Contract Renewals and Service Add-Ons

Additions to your contact center solution can be purchased at any time. Feature additions and carrier service changes may require a contract addendum.

- **Feature Add-On's –** Contact your assigned Genesys Account Manager
- **PureConnect Cloud Edition Upgrade –** Contact your assigned Genesys Account Manager
- **Contract Renewal –** Contact your assigned Genesys Account Manager
- **Telco Services –** Please open a support case to request one or more of the following (examples):
    - Additional toll-free numbers
    - Additional DID/DDI's
    - Increase / decrease of call ports
    - Resporg of numbers
    - Calling name (CName) party changes
    - Vanity numbers
    - Rerouting of numbers
- **MPLS Services** – Please open a support case to request one or more of the following changes (examples):
    - Bandwidth increase / decrease
    - QoS Updates
    - Additional site terminations
- **Data Center Hosting –** Please open a support case to request one or more of the following changes (examples):
    - Additional rack units
    - Additional cross connects
- **Agent Limit –** The price and service package set forth in the applicable Services Order is subject to change in our sole discretion if your actual use exceeds the limit (600 agents for Standard Edition, or 6,000 agents for Preferred and Premium Editions) in two (2) of any three (3) consecutive months. Enterprise customers may burst above their minimum commit at any time subject to the Bursting Premium pricing. If the customer bursts for 3 or more months above the Bursting Allowance or any single month of 2,000 additional users, then the customer must enter into an amendment to the Services Order to increase their minimum commit. A single deployment of PureConnect is capped at 10K agents and 20K configured users. Bursting above that limit will void SLAs.

# PureConnect Cloud Policies

## Major Version Upgrades

Major version upgrades of Genesys software are included free of charge with your service. Our Services team will schedule and plan all major version upgrades individually, to ensure the timing of the upgrade is acceptable, and that any unique customer requirements are met. Requests for major version upgrades can be made once the new release is available. Please open a support case to request your next major version upgrade. The Services team will provide all commercially reasonable efforts to honor requests for major version upgrades outside of the normal process.

## Release Updates

Release updates of the Genesys software are included free of charge with your service. Release updates are applied for a variety of reasons such as access to new features, more than three (3) updates behind the current Generally Available (GA) update, and software defect issues. Typically, you should expect a single release update once per year (or as necessary). You may request updates to the latest release update. However, these requests may not always be honored if the following criteria have not been met:

- A release update has already been applied within the current quarter
- There are no system impacting issues driving the request

When a release update is installed, all open support cases that are to be resolved by the update will be closed. Support cases will also be referenced in a new case after the installation of the update.

## Service Support

At least two (2) staff members are required to become designated contacts in order to access Genesys' Support department. Designated contacts are encouraged to take the PureConnect Cloud Certified Professional certification is aimed to educate your staff on the PureConnect platform and enable them to do their own Level 1 support (see definition in the Support Policy attached to the Genesys Master Subscription Agreement). Should you prefer not to do your own Level 1 support, you may choose a Genesys Elite Partner for these services.

## VoIP Ready Network

As a part of your service contract with Genesys we require your network meet the following standards:

- Quality of Services (QoS) must be enabled on all VoIP-related network devices, endpoints, and configured in accordance with the QoS for the xIC Platform whitepaper.
- Full duplex must be enabled on all network devices.
- RTP latency, in one direction, must be less than 150 ms for voice traffic.
- RTP jitter must be less than 30 ms.
- RTP packets must include highest markings for service priority queuing (e.g. DSCP for Cisco devices).
- Network segments must not exceed a packet loss rate of one percent (1%).
- Network bandwidth must accommodate approximately 88kb/s for calls using audio codec G711 and 32kb/s for calls using audio codec G729 (not including overhead for VPN encryption/decryption if applicable).
- VLAN settings must be set in accordance with the QoS for the xIC Platform whitepaper published at the time of this agreement.

If Genesys determines that your network does not meet these standards, you must rectify the failures. You will not be entitled to receive Hard Outage credits until your network meets these standards.

## Change Control

All changes made by Genesys employees to live service customers are required to follow our established Change Management Process. Our formal change management process ensures that we abide by a managed and orderly process by which such changes are requested, approved, communicated (if possible), logged and tested. All changes, including MACs, to core infrastructure, operating systems, core applications, and ancillary applications follow this process.

## Access Control

Our Access Control policy, based on least privilege required, strictly governs access to all underlying components of your service. Adds, changes, and deletions of access accounts must be performed in a controlled and traceable manner. All access control requests are submitted to the NOC, with a completed Access Control form, which then requires approval by management prior to implementation.

## Security Policies, Procedures & Guidelines

All Genesys team members supporting your service are required to follow policies, procedures and guidelines detailed within our Information Security Management System (ISMS). Acknowledgement and conformance is required by each team member prior to gaining access to any component used in the delivery of your service.

## Security Incident Response

Genesys has deployed a cross-disciplinary Security Incident Response Team (SIRT) that is responsible for responding to any potential or identified security incidents pertaining to your service. If you suspect a security incident please do not hesitate to open a case with Support or submit an email directly to SIRT@genesys.com.

## Vulnerability and Patch Management

Genesys has deployed a Vulnerability Management team that includes members of the Security, Operations and Engineering teams, to manage and mitigate security vulnerabilities of your service. The Vulnerability Management team also works closely with the Genesys Testing team to make sure that all patches are functionally tested before being deployed to your service delivery components.

## Protection against Malicious and Mobile Code

Detective, preventive, recovery, and appropriate user awareness controls and procedures have been implemented to protect against the installation of malicious code to your service delivery components. All Service team members have been trained on the risks associated with obtaining files from or via external networks.

## Data Privacy

Genesys is committed to safeguarding the personal information that we store on behalf of our customers. Protected information, such as Non Public Personal Information (NPPI), will only be used for the purpose of performing our contractual obligations of your service. Appropriate administrative, technical, and physical safeguards have been implemented to prevent the use or disclosure of protected information. These measures also ensure the integrity and availability of the electronic protected information that we receive, maintain, and transmit as a part of your service. In the event of a security breach the Security team will communicate with customers within two (2) days of a confirmed unauthorized disclosure of Protected Information (PI).

## Data classification

Our Security team assigns data classification, to all data types, generated to ensure that all data is consistently protected throughout its lifecycle in a manner commensurate with its sensitivity level. Data classification matrices are constructed and reviewed annually by the Security team.

## Password Policies

Below is a list of our general guidelines for PureConnect user account password creation. These guidelines are PureConnect Cloud default policies for general security and preventive measures against toll fraud.

- **Maximum number of unique passwords before one can be reused: 10**
- **Minimum age of password before user can change it (days): 2**
- **Maximum password age (days): 90**
- **Password age warning period (days before password expires): 14**
- **Minimum password length: 8**
- **Minimum number of unique DTMF digits: 4**
- **Allow all sequential digits: remains unchecked**
- **Password must not be the same as extension (or extension + extension)**
- **IC passwords should not include special characters as these are not recognized by the Telephony User Interface (TUI)**
- **Maximum number of failed login attempts = 5**
- **Lockout duration = 15 minutes**
- **Failed login reset time = 15 minutes**

Changes to the default password policy may be accommodated through the execution of a contract addendum.