AAPT

Cloud Contact Centre Technical Requirements

Document Number: 221-10100-CG-2

Issue :1.0

Date: January 2013

Contents

Overview of Configuration Requirements

The primary requirements to use the Cloud Contact Centre are:

- a personal computer with a web browser
- a business grade high-speed connection to the Internet
- a telephone device

In a typical small business and at home setups, you can open your browser, login to the Cloud Contact Centre services site and gain full access to the service.

In larger business environments you may be required to configure various browser and network permissions and security policies to allow full access to Cloud Contact Centre features.

This document discusses technical details of system and network capabilities required to support all features of the Cloud Contact Centre application.

You must configure both your network and agent workstations to successfully interoperate with Cloud Contact Centre.

In most networks, the only required configuration tasks are to enable Cloud Contact Centre to :

- Retrieve email messages from your organization's email server
- Enable Agent Console to access the Cloud Contact Centre platform assigned to them

In networks with aggressive security policies, you may also need to selectively enable access for specific IP addresses and associated firewall ports used by Cloud Contact Centre.

For each agent workstation supported by the Cloud Contact Centre, you must provide the agent with appropriately configured network, computer, and telephony equipment.

Network Configuration Requirements

This section describes how to configure the following network components to interoperate with Cloud Contact Centre:

- Your email server
- Your firewall or other network address translation (NAT) equipment
- The Collaborate Feature.

Enabling Cloud Contact Centre to Retrieve Email

Cloud Contact Centre supports the POP3 / POP3 SSL and IMAP / IMAP SSL email protocols.

The only inbound network access required by the Cloud Contact Centre are the ports used to retrieve email from your organization’s email server. If your network uses only a third party email host such as AOL, Yahoo, or Gmail, you do not need to open firewall ports to support email access.

When retrieving email from your existing email server, Cloud Contact Centre submits the username and password for a mailbox.

- For POP3 email support, enable port 110.
- For POP3 SSL, enable port 995.
- For IMAP email support, enable port 143.
- For IMAP SSL, enable port 993.

If your network uses non-default email ports, in the Configuration Manager, use the **Email Channels** page, **Properties** tab, to specify the non-default port numbers.

Enabling Outbound HTTP/HTTPS Communications

The only outbound network access required by the Cloud Contact Centre are TCP ports 80 and 443, used for HTTPS communications with each Agent Console.

Selectively Enabling IP Addresses and TCP Ports

In networks that block unknown IP addresses and ports by default, you may need to selectively enable the IP addresses and TCP ports used to access your Configuration Manager and Agent Console.

Your Cloud Contact Centre representative will provide you with the URL you will use to access your Configuration Manager. You can then use that URL information to enable the associated IP traffic to pass through your network's firewall.

Enabling Call Recording FTP Requirements

To enable downloading of call recordings from your Cloud Contact Centre tenant, you must use a FTPS client. We validates the use of the following FTPS client.

- Core FTP LE, available from http://www.coreftp.com/

Your Cloud Contact Centre representative will provide you with the URL you will use to access your FTP Server.

You must also open the following outbound ports on the firewall with IP address of the specific ftp server(e.g. ftps.mycontactual.com for United States):

- TCP: 21(FTP)
- TCP: 30000 – 30999

Collaborate Technical Requirements

The optional Collaborate feature in Cloud Contact Centre enables agents to connect to a customer computer for purposes of providing hands-on assistance.

To enable an agent to use the Collaborate feature, and a customer computer to run the Collaborate feature:

- Configure both the agent's and customer's computer to allow traffic to pass through TCP port 5907. If an agent's or customer's computer is behind a corporate firewall, the firewall must also permit the Collaborate feature to use TCP Port 5907.
- Verify that the customer computer includes a Java Runtime Environment (JRE).
- Configure the anti-virus software and operating system security features on the customer computer to permit the download and running of the Collaborate program.

- Some anti-virus programs or operating system security features may incorrectly
- identify the program downloaded to the customer's computer by the Collaborate feature as a security threat.

Overview Of Agent Technical Requirements

Each Cloud Contact Centre agent requires:

- A properly equipped and configured computer.
- A high-speed network connection.
- A telephone device.

Depending on the types of transactions being managed by the Cloud Contact Centre, an agent workstation may also require additional equipment or configuration steps.

Agent Network Connectivity Requirements

All Cloud Contact Centre agents, supervisors, and administrators must have high speed Internet access. Examples of high speed Internet include DSL, Cable, or most corporate LANs. We strongly recommends the use of a business grade internet access and where possible this should be dedicated to Cloud Contact Centre.

For Agent browser traffic networks are required to have the following characteristics:

- Low latency with average of less than 100 ms
- Low or negligible packet loss
- Allocation of 100Kb per sec / agent session

Although Cloud Contact Centre can interoperate with high-speed satellite connections, the round-trip transmission delay inherent in all satellite connections will probably result in an undesirable degradation in performance. It is also preferable that Agents using this service are located in Australia to avoid latency issues.

Dial-up Internet connections are not supported.

Agent Firewall Requirements

- Cloud Contact Centre works with typical default stateful inspection firewall settings.

- Cloud Contact Centre requires standard NAT with any VoIP Application Layer Gateway (ALG) address fix up features disabled.
- The Cloud Contact Centre browser and Cloud Telephony phone sessions periodically generate activity to keep stateful inspection ports open.
- For organizations with restrictive firewall settings, Cloud Contact Centre recommends stateful inspection to open the following ports automatically when needed:
    - Agent browser session uses ports 80 and 443.
    - Collaborate feature uses port 5907.
    - Downloading call recordings through FTPS clients uses port 21 and ports in range 30000-30999.

Agent Computer Hardware and Software Requirements

Computer Hardware

- Agents require a personal computer and a high speed Internet connection capable of running Microsoft Internet Explorer (version 7, or higher recommended) quickly when accessing popular search sites such as Google and Yahoo.
- If an agent uses a Cloud Telephony soft phone then the agent's computer and Internet connection must consistently perform well while processing all other desktop applications required by an agent.
- Agent screens must support a resolution of no less than 1200x900 pixels . Higher screen resolution is recommended.

Java

If the Agent *Collaborate* feature is enabled, then the computer running the Cloud Contact Centre must include a Java Runtime Environment (JRE).

Agent Browser Configuration Requirements

Cloud Contact Centre supports the following versions of Internet Explorer:

- Internet Explorer 6, 7, 8, and 9

Note: Support for Internet Explore versions 6, and 7 will end following the next major release of Cloud Contact Centre (version 7.0). Our next release scheduled for 2013 will support IE8 and IE9 only.

Browsers other than Internet Explorer may fail to support one or more essential features of Cloud Contact Centre.

Note: Cloud Contact Centre is partially compatible with Firefox and Safari offering support to Agent Console - Control Panel functionality, however, we does not recommend the use of these browsers with the service.

Managing Agent Browsers and Security Zones

You may need to configure Internet Explorer to enable you to work with all Agent Console features.

Internet Explorer places Web sites in one of four security zones:

- Internet (most trusted, least strict security settings)
- Local intranet
- Trusted sites
- Restricted sites (least trusted, strictest security settings)

When you assign a site's URL to an Internet Explorer security zone, you are specifying the security settings that Internet Explorer uses when you visit that site. Depending on your call Centre's security policies, if you are an Agent Supervisor, in Internet Explorer you will add the URL of your Agent Supervisor Console to either the *Internet* or *Trusted sites* zone.

If Cloud Contact Centre updates the URL of your agent or agent supervisor desktop, you will then need to update your Internet Explorer settings in response to that change. More specifically, you will:
1. Remove the old URL from its security zone
2. Add the new URL to the zone.
3. Configure the new URL's security settings

Configuring Internet Explorer

The configuration requirements for Internet Explorer differ slightly, depending on:

- Whether the agent account type is Agent or Agent Supervisor
- Which version of Internet Explorer the Agent or Agent Supervisor account uses

The table below lists the Agent Desktop account and supported Internet Explorer versions, and specifies the configuration tasks you must perform for different combinations of account type and browser version.

Agent	Supervisor	Task
X	X	For both Agent and Agent Supervisor accounts, in Internet Explorer 8, you must disable Internet Explorer's SmartScreen Filter feature. **To disable Internet Explorer 8 SmartScreen Filter for both Agent and Agent Supervisor accounts:** 1. In **Tools** choose **Internet Options**, then click the **Advanced** tab. 2. In the **Advanced** tab, in the **Security** area clear the **Enable SmartScreen Filter** check box to disable the feature.
	X	For Agent Supervisor accounts, in all supported versions of Internet Explorer, you must disable file download prompting. **To disable Internet Explorer download prompting for Agent Supervisor accounts:** 1. In **Tools** choose **Internet Options**, then click the **Security** tab. 2. In the **Security** tab, choose the **Internet** or **Trusted site** zone. For information about security zones, see the section *Managing Agent Browser Security Zones.* 3. In the **Security** tab, click **Custom Level**, then in the **Download** section enable **Automatic Prompting for File Downloads**.
X	X	For Agent and Agent Supervisor accounts that use CRM integration, including Salesforce and NetSuite, in all supported versions of Internet Explorer, you must disable pop-up blocking and all Internet accelerators. **To disable Internet Explorer pop-up blocking and accelerators for Agent and Agent Supervisor accounts that use CRM integration:** 1. In **Tools**, choose **Pop-up Blocker**, then choose **Turn Off Pop-up Blocker**.

		2. In **Tools**, choose **Manage Add-ons**, then in **Accelerators** right-click each accelerator and choose **Disable**

Agent Telephone Connection and Equipment Requirements

To receive telephone calls from the Cloud Contact Centre application, agents must have access to one of the following types of telephone connection:

- Public switched telephone network (PSTN) connection
- Cloud Telephony connection

For both Cloud Telephony or PSTN telephones, the telephone assigned to the Cloud Contact Centre must:

- Always be available to receive incoming calls.
- Not forward calls to a non-Cloud Contact Centre voice mail box before the Cloud Contact Centre can offer an incoming call to an agent, and forward that call to an agent's Cloud Contact Centre voice mail box if no agent accepts the call.

Agent PSTN Equipment Requirements

Public Switched Telephone Network (*PSTN*) telephone connections:

- Can be directly accessed by dialing a Direct-Inward Dialing (DID) phone number
- Must not prompt or otherwise require a caller to dial a separate extension number

The Cloud Contact Centre supports the following types of PSTN equipment:

- A telephone connected to a conventional telephone wire (“landline”)
- A mobile phone
- A direct-access IP phone

Agent Cloud Telephony Telephone Requirements

NEC Cloud Telephony connections use a data connection to originate and transport telephone calls.

The Cloud Contact Centre supports the following types of VoIP telephone equipment:

- Software based VoIP phones such as the CounterPath eyeBeam Basic softphone
- Hardware based VoIP phones such as the NEC DT700 and Polycom Soundpoint series IP Phone

Agent Voice Headset Selection Guidelines

When evaluating agent VoIP headsets, always choose Contact Centre professional-quality equipment manufactured by companies such as Plantronics or Jabra-GN NetCom.