inContact

Hosted

Customer Site Requirements for inContact Workforce Optimization 16.3

www.incontact.com

Customer Site Requirements for inContact Workforce Optimization

- **Version** — 16.3
- **Last Revision** — October 2016
- **About inContact** — inContact (NASDAQ: SAAS) is the cloud contact center software leader, with the most complete, easiest, and most reliable solution to help organizations achieve their customer experience goals. inContact continuously innovates in the cloud and is the only provider to offer a complete solution that includes the customer interaction cloud, an expert service model, and the broadest partner ecosystem. Recognized as a market leader by Gartner, IDC, Frost & Sullivan, Ovum, and DMG, inContact supports over 6 billion interactions per year for enterprise, midmarket, government organizations, and business process outsourcers (BPOs) who operate in multiple divisions, locations, and global regions. To learn more about inContact, visit www.incontact.com.
-
- **Disclaimer** — inContact reserves the right to update or append this document, as needed.
- **Contact** — Send suggestions or corrections regarding this guide to the technical documentation team at documentationsrequest-discover@incontact.com.

Introduction

Audience

This document is written for customers and prospective customers interested in using inContact WFO in the cloud. Readers should have a basic level of familiarity with general networking and their organization's LAN, the inContact PBX, the business rules in their contact center(s), usage of a PC and its peripherals, and the Windows operating system.

Goals

The goal of this document is to provide knowledge and reference information necessary to support deployment and configuration of an inContact WFO system in an organization's IT environment.

While the majority of components and modules reside in the inContact Cloud, certain services may need to reside on a server or servers at your location(s) if the deployment includes inContact Screen Recording.

> **Note:**
> This document is NOT intended as a specific system or network design document, nor is it designed to educate the reader on contact center concepts or best practices.

Assumptions

This document assumes the reader has access to an inContact WFO Sales Engineer, Project Manager, or other resource to assist in applying this information to the reader's environment.

Need-to-Knows

inContact WFO is a robust, cloud-based platform with multiple modules that can be used alone or in any combination with each other. These modules include:

- inContact Call Recording
- inContact Screen Recording
- inContact Quality Management
- inContact Workforce Management v2
- inContact Desktop Analytics

This document covers requirements for inContact WFO systems that include one or more of the following: inContact Call Recording, inContact Screen Recording, inContact Quality Management, inContact WFMv2 and inContact Desktop Analytics.

Server Requirements

Warning:

The specific hardware and system software required for your implementation is determined by inContact WFO Sales Engineering during the discovery and system design process. No system hardware or software should be purchased or requisitioned until the final system design document is complete.

Hardware Requirements

An on-premises server (known as the PREMISES Server) is required *only* if you are using inContact Screen Recording. This server must have a public-facing IP address.

In general, inContact recommends a server with at least 6 GB of RAM and a quad-core processor. The server can be either physical or virtual.

The PREMISES server should be built using this drive configuration:

Drive Letter	Drive Purpose	Size
C:	System	50 GB
D:	Applications	20 GB
E:	Storage	TBD

An on-premises server (known as the PREMISES Server) is required. This server must have a public-facing IP address. Hardware requirements may also be affected by the specific inContact WFO components used, the number of agents being recorded, and the design of your telephony network.

Generally speaking, servers can be either physical or virtual. Some recording integrations require physical servers; see the Overview topic or customer guide for your integration.

Software Requirements

The following software environments have been tested with and are supported for system servers:

- **Operating System** — Windows Server 2012 R2. Integration with Avaya using IP Office requires a recording server running a 32-bit Windows operating system. See the *Customer Guide to Avaya IP Office Integrations* for details.

- **Operating System** — Windows 2012 R2
- **Protocols** — IPv4

Prerequisites

The inContact WFO deployment team will install and configure the software on the PREMISES Server. In addition to the inContact WFO software, they will also install the following prerequisites:

- .NET Framework v3.5, v4.0, v4.5.1, v4.5.2, and v4.6.1
- Microsoft Visual C++ Runtime v8.0.50727.4053 (for more detail on this software, see knowledgebase article 973544 on Microsoft's support site)
- Microsoft PowerShell v2.0 or greater (for more detail on this software, see knowledgebase article 968929 on Microsoft's support site)
- Windows Installer v4.5 or greater
- Microsoft Report Viewer Redistributable 2008, 2010, and 2012 (for more detail on this software, see knowledgebase article 971119 on Microsoft's support site)
- A self-signed SSL certificate to enable secure communication between the PREMISES Server and the cloud

Licensing

inContact WFO Sales Engineering explains licensing requirements during the sales process. If SSL is used in the network, a certificate file must be purchased from a third-party vendor (such as VeriSign). SSL is recommended for systems that include a PREMISES server..

PC Requirements

The following requirements apply to workstations using the inContact WFO Web Portal as well as those running inContact Screen Recording or inContact Desktop Analytics client applications.

Software Requirements

For complete information on supported client operating systems and browsers, see Supported Environments.

inContact WFO offers two options for recording search and playback. The **Call List** and **Web Player** (also known as the Silverlight Player) are supported in the following browsers: Internet Explorer and Firefox only. The **Interactions List** and **HTML5 Interaction Player** are supported in the following browsers: Chrome and Firefox only.

> **Note:**
>
> The HTML5 **Recorded Interactions** list does not yet support live monitoring or speed-adjusted playback. It also does not support manual blackouts.

Users who play call recordings, screen recordings, or both, and who use the Silverlight Player, also need:

- Microsoft Silverlight browser plug-in v5.0.61118.0 or higher

If your deployment includes inContact Desktop Analytics, a proprietary client application must be installed on each PC used by recorded agents. This PC must also run:

- .NET Framework v4.5.2

If your deployment includes screen recording, a proprietary client application must be installed on each PC to be recorded. This PC must also run:

- .NET Framework v4.0

Hardware Requirements

The minimum workstation specifications for users who simply view information in a web portal are:

- 2.0 GHz Processor
- 1 GB RAM
- 50 MB hard drive space
- 1280 X 800 (minimum screen resolution at 16-bit color depth)

Users who monitor calls, screen activity, or both; who perform quality evaluations; or who in general use the web portal more heavily will normally benefit from more powerful PCs. For these users, inContact recommends:

- 3Ghz or 1.6Ghz dual core
- 2 GB RAM
- 50 MB hard drive space
- 1280 X 1024 or higher screen resolution at 16-bit color depth

Virtual Desktop Infrastructure (VDI) Support

inContact WFO supports the following virtual desktop systems:

- Microsoft Terminal Services
- Citrix XenDesktop
- VMWare View

inContact WFO does not support Citrix XenApp in application streaming mode for any applications. However, if the endpoint launching the XenApp client is a Windows PC, the inContact Screen Recording client will capture the streamed application windows ***if*** the client is running on the Windows PC itself.

> **Note:**
> VDI does not affect call recording.

MAJOR CONSIDERATIONS

Each application instance in use will consume resources on the customer's VDI. The following table provides some general guidelines regarding resource usage for each inContact WFO application or module; however, inContact strongly recommends testing needed resources by deploying desired applications and modules to a limited number of users and evaluating resource utilization in your specific environment.

inContact WFO Module	Estimated Resource Usage
inContact Screen Recording Client	RAM: 50-250MB, CPU: 1-5% per instance (highly dependent on screen resolution and activity)
Web Player (browser-based Silverlight application)	RAM: 50-500MB, CPU: 1-10% per instance (highly dependent on number of records returned by user queries and size of audio/video files being played)

inContact Desktop Analytics Client	Resource usage can vary greatly depending on the type and number of applications being monitored, which scripts are being used, and so on. Requires testing in customer's environment to determine specifics.

The inContact WFO **Web Player** may play back data recorded in full HD (in other words, at resolutions greater than 1080p) and the size of the recordings may be significant.

Each VDI vendor has specific caveats and limitations regarding performance for media playback, and most have specific considerations for Silverlight-based media players, especially if the endpoint is a thin or zero client. Consult your vendor for specific information regarding your deployed products.

Note:

Microsoft offers a publicly-available Silverlight media player demo application you can use for initial performance testing. Visit Microsoft's iis.net website and search for IIS Smooth Streaming.

Environmental Requirements

inContact WFO cloud servers have IP addresses in the following range: 207.166.100.0/23.

Port Information

To minimize the number of ports that must be opened in your firewall, inContact WFO uses a service called **Connection Pooling** on the PREMISES server. This service requires:

Port	Transport	Description
2010	HTTP(S)	Open on server and firewall for communication between the PREMISES server and the cloud. Either HTTP or HTTPS can be used. HTTPS is used by default. Talk to your team if you have questions about secure transport configuration.

In addition, the following ports must be open at your location to allow for proper communication between inContact WFO components:

Port	Transport	Description
4510	TCP	Connections from Silverlight client players
2020	HTTP	inContact WFO Web Portal connections using the HTML5 Interaction Player
5650	HTTP	Token requests for the HTML5 Interaction Player
443	HTTPS	HTTP services on the client PCs for inContact WFO Web Portal
943	TCP	Silverlight cross-domain policy listener
5638	TCP	Logging communications between client PCs and the PREMISES server
5672	TCP	Used by the messaging interface for various inContact WFO services

If you use inContact Screen Recording, you will additionally need:

Port	Transport	Description
5633	TCP	Open on client PCs for communication between the PC and the PREMISES server. Secure communication between the PREMISES server and the clients is dependent on the security of your LAN.

If you use inContact Desktop Analytics, you will additionally need:

Port	Transport	Description
5634	TCP	Open on client PCs for communication between the PC and the PREMISES server. These communications can be secured using HTTPS and SSL. For more information, talk to inContact Support or see our online help at inContact WFO Admin>Security and Desktop Analytics.

Antivirus Software

Antivirus exclusions should be configured in any system where antivirus scanning is installed. The guidelines below are provided to assist with ensuring the reliability and performance of your inContact WFO system, while still providing for a secure environment. A lack of exclusions can cause system performance issues and possibly contribute to service outages.

These guidelines apply to both memory resident and on-demand scanning.

GENERAL CONSIDERATIONS

These exclusion guidelines are product-specific. For applications not specifically listed, it is often necessary to determine exclusions on a case-by-case basis. This section provides guidance in this area.

Files should typically be excluded based on the following criteria:

- **Locked Files** — The files are permanently locked open by a legitimate server process. Examples of these are databases such as DHCP and SQL Server, as well as files such as the Windows Pagefile.
- **Large Files** — The files are manipulated often by a legitimate server process and are typically large in size. Examples of these are copying CD/DVD images (.iso) and Virtual Machine Files (.vhd). In addition, operations may include offline maintenance on Virtual Machine Files and Exchange Server databases.
- **Temporary Files** — A large number of temporary files are written to disk by a legitimate server process.

EXCLUSION GUIDELINES

The following should be excluded from anti-virus scanning on the PREMISE Server:

- The cc_screencapserver.exe process
- Files with the *.vid extension
- The default folder associated with inContact Screen Recording, C:\temp\
- The cc_loggerservice.exe process
- Files with the *.log extension
- The default folder associated with inContact WFO logging, C:\Program Files\CallCopy\Logs\