

# ContactPro Mobile App

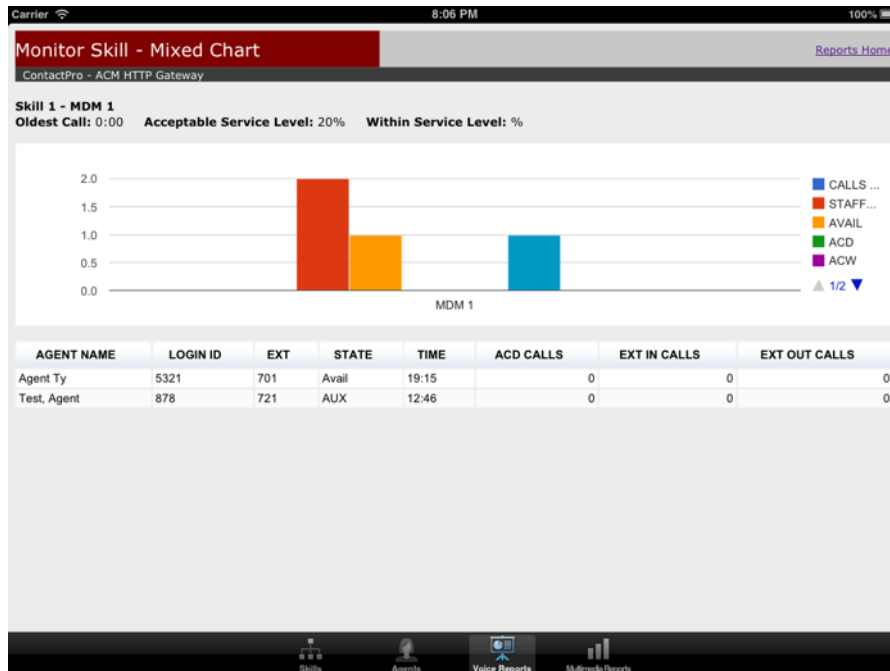
Fact Sheet



## CONTACTPRO MOBILE APP

ContactPro Mobile App is an iOS App solution to provide customers reporting and skilling functionality through mobile and tablet devices. The solution is currently available for Apple iOS.

This solution brings the benefits of modern and flexible reporting to the end user to get an overview about the status of your contact center.



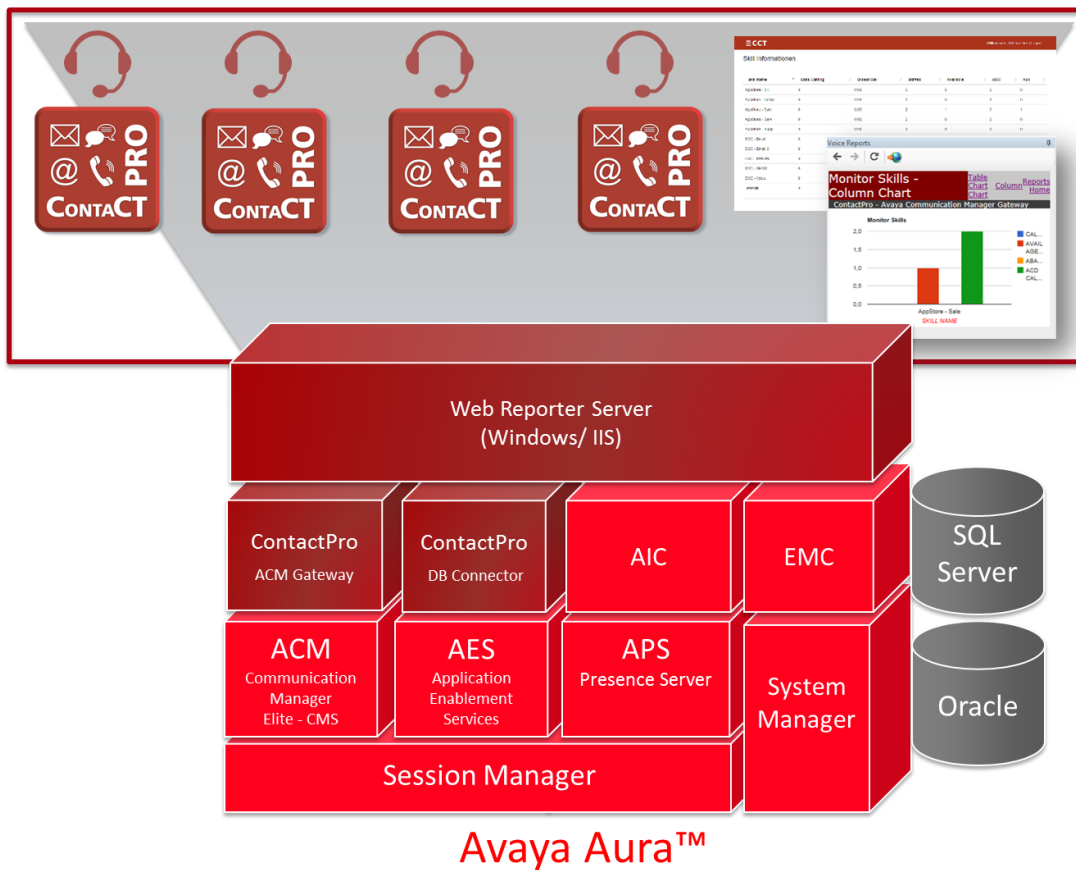
### Features:

- ☰ Connection to different reporting sources
- ☰ Avaya Communication Manager / BCMS Interface
- ☰ Consolidated reports
- ☰ Skilling functionality for Voice skills
- ☰ User-friendly configuration and administration

The solution is using the iOS Developer program modern ASP .Net environment to ensure the flexibility and performance at the mobile device.

Used developing tools:

- ≡ Hosting: Microsoft Internet Information Service IIS
- ≡ Server-Script: iOS Developer program, ASP .Net
- ≡ Server-Frameworks: ASP.NET MVC, Entity Framework, .NET
- ≡ SQL Database for configuration data: SQL Express, SQL Server Standard or SQL Server Enterprise



Prerequisites to connect the mobile app to the customer environment:

- ≡ Apple iPhone or Apple iPad with iOS 5 or above
- ≡ Avaya Communication Manager R6 or higher
- ≡ CCT ACM Gateway R2 or higher
  - OS:
    - Ubuntu Linux 14 or above
    - Debian 7 or above
    - Red Hat Enterprise Linux 5.4 or above
  - 2,4 GHz Dual Core
  - 2 GB RAM
  - 15 GB HDD
  - Hard disk drive with at least 7200 rpm rating
  - 512 KB L2 cache
  - 100 BaseT Ethernet NIC, which can either be locked to 100M / full or use Auto–Negotiation to achieve 100M / full
  
- ≡ Reporting Server
  - OS:
    - Windows 2008 R2
    - Windows 2012 R2
  - Microsoft IIS 7 or above
  - Database
    - SQL Server Express
    - SQL Server Standard
    - SQL Server Enterprise
  - 2,4 GHz Dual Core
  - 2 GB RAM
  - 10 GB HDD
  - Hard disk drive with at least 7200 rpm rating
  - 512 KB L2 cache
  - 100 BaseT Ethernet NIC, which can either be locked to 100M / full or use Auto–Negotiation to achieve 100M / full

The CCT App supports the following connection methods through the mobile device:

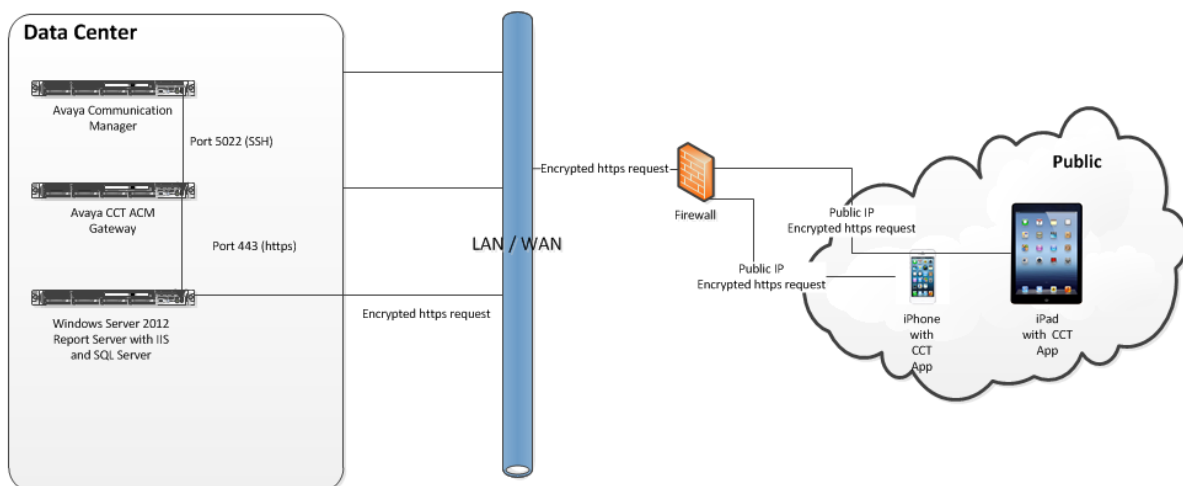
- ≡ Connection through configured WLAN of mobile device for internal use in the network of the customer
- ≡ Connection through public IP with firewall access
- ≡ Connection through VPN client configured on the mobile device

For all connections, the CCT App uses the configured settings in the iOS. There is no integrated WLAN or VPN configuration inside the App.

The CCT App supports a two-factor authentication through username and password configured on the reporting server and the mobile device id.

The following example shows the demo configuration for the CCT App:

#### CCT Mobile App Network Architecture



The CCT App creates an encrypted https request to the public IP of the firewall. The firewall grants the access to the rules and forwards the https request to the reporting server. The reporting server checks the authentication of the request, if allowed the reporting server manages the handled reporting, and skilling requests to the CCT ACM Gateway, which collects the necessary data from Avaya Communication Manager. All the data will be encrypted and sent back to the mobile App to display the reporting results.

Copyright © 2015 CCT

Transmission and reproduction of these documents to utilize or disclose its contents are not permitted unless explicitly granted. Offenders are liable to pay damages. All rights reserved.

**Issued by:**

CCT Deutschland GmbH  
Heinrich-Hertz-Strasse 5  
60486 Frankfurt am Main  
Germany  
Tel. +49 69 7191 4969 0  
contact@cct-solutions.com

CCT Software LLC  
1735 Market Street STE 3750  
Philadelphia, PA 19103  
United States of America  
Tel. +1 267 507 6196  
contact@cct-solutions.com