



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Teleopti WFM with Avaya IP Office Contact Center – Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for Teleopti WFM to interoperate with Avaya IP Office Contact Center. Teleopti WFM is a work force management solution.

In the compliance testing, Teleopti WFM used the Web Service Collection interface from Avaya IP Office Contact Center to monitor real-time agent states, for analysis and display of agent states and adherence against planned schedules.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the configuration steps required for Teleopti WFM to interoperate with Avaya IP Office Contact Center. WFM is a work force management solution.

In the compliance testing, WFM used the Web Service Collection (WSC) interface from IP Office Contact Center to monitor real-time agent states, for analysis and display of agent states and adherence against planned schedules.

The DirectoryWS web service of WSC is used by WFM to obtain basic and detail information on agents, and the MonitoringWS web service is used by WFM to monitor agents' working and logging states.

The IP Office Contact Center configuration included connection to an IP Office Server Edition environment consisted of two IP Office systems, a primary Linux server and an expansion IP500V2 that were connected via Small Community Network (SCN) trunks.

## 2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the WFM application, the application established WSC connectivity to IP Office Contact Center for obtaining agent information and for requesting agent monitor.

For the manual part of the testing, each call was handled manually on the agent desktop running the IP Office Contact Center User Interface to alter agent states.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to WFM.

The verification of agent states included viewing of the reported agent states over the WFM web interface. For simplicity, the testing did not include creation of agent schedules.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between IP Office Contact Center and WFM utilized the enabled capabilities of TLS.

## 2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on WFM:

- Use of WSC DirectoryWS web service to obtain agent basic and detail information.
- Use of WSC MonitoringWS web service to monitor agent working and logging states.
- Proper reporting of agent states for scenarios involving log in, log out, on/off break, after call work, inbound, outbound, internal, external, personal, hold/reconnect, transfer, conference, multiple agents, long duration, and outbound campaign.

The feature testing included agents on both IP Office systems.

The serviceability testing focused on verifying the ability of WFM to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to WFM.

## 2.2. Test Results

All test cases were executed and verified.

The one observation on WFM is that by design, all agent states were initially reported as **Ungrouped states** by default. WFM required all desired agent states to manually occur and therefore captured by the application, before the administrator can configure the preferred reporting of such states.

## 2.3. Support

Technical support on WFM can be obtained through the following:

- **Phone:** <https://www.teleopti.com/wfm/about/contact/contact-me.aspx>
- **Email:** [servicedesk@teleopti.com](mailto:servicedesk@teleopti.com)

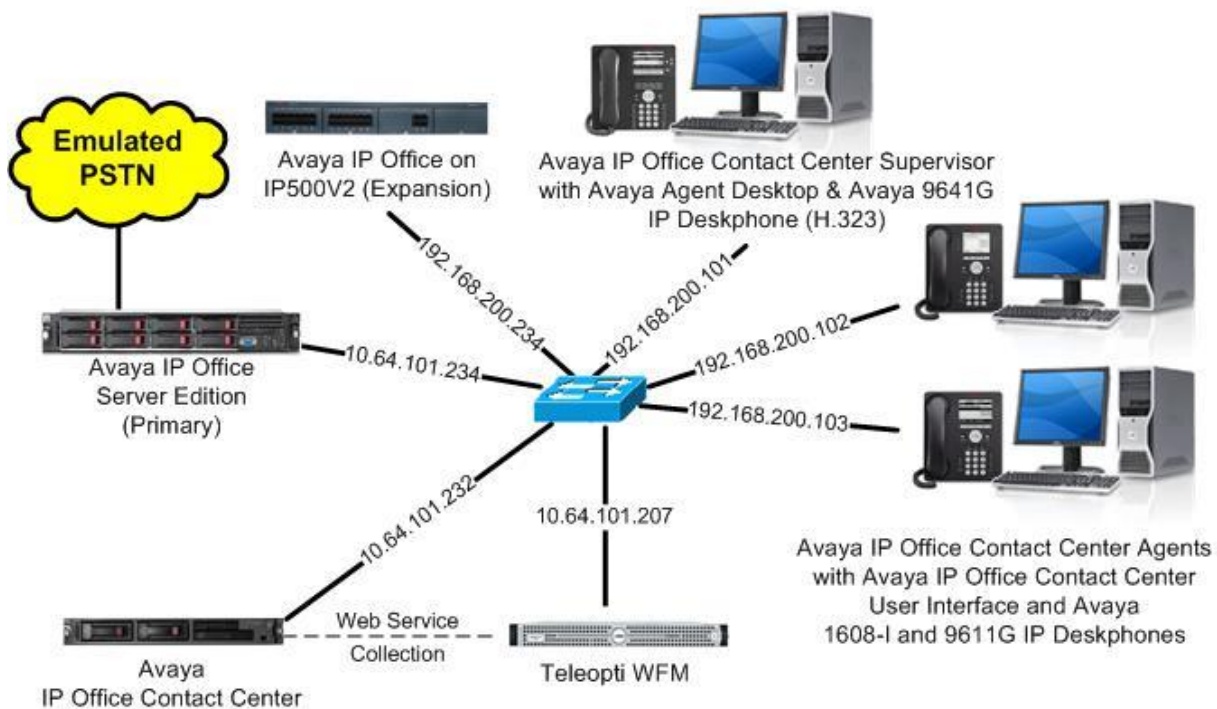
### 3. Reference Configuration

WFM can be configured on a single server or with components distributed across multiple servers. The compliance testing used a single server configuration, as shown in **Figure 1**.

The detailed administration of basic connectivity between IP Office Contact Center and IP Office, and of contact center devices is not the focus of these Application Notes and will not be described.

The contact center devices used in the compliance testing is shown in the table below. In the testing, WFM monitored all agents shown below.

Contact Center Devices	Values
Supervisor User	37880
Agent Phones	21031, 22031
Agent Users	37881-4
Agent Names	Agent1-4



**Figure 1: Compliance Testing Configuration**

## 4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya IP Office Contact Center	10.1.0.0
Avaya IP Office Contact Center User Interface on Windows 10	10.1.0.0
Avaya IP Office Server Edition (Primary) in Virtual Environment	10.1.0.0.0
Avaya IP Office on IP500 V2 (Expansion)	10.1.0.0.0
Avaya 1608-I IP Deskphone (H.323)	1.3110
Avaya 9611G & 9641G IP Deskphone (H.323)	6.6506
Teleopti WFM on Windows Server 2012 <ul style="list-style-type: none"><li>• Web</li><li>• Log Server</li><li>• Microsoft SQL Server 2017</li></ul>	8.6.504.50953 R2 Standard 8.6.504.50953 7.2.1.74979 RC1

*Compliance Testing is applicable when the tested solution is deployed with a standalone IP Office 500 V2 and also when deployed with IP Office Server Edition in all configurations.*

## 5. Configure Avaya IP Office Contact Center

This section provides the procedures for configuring IP Office Contact Center. The procedures include the following areas:

- Launch Administration
- Verify license
- Launch User Interface
- Administer agents
- Administer registry
- Restart services

The Certificate Authority root certificate and the IP Office Contact Center server identity certificate are assumed to be pre-installed on the IP Office Contact Center server.

### 5.1. Launch Administration

From the IP Office Contact Center server, access the Administration web-based interface by using the URL “https://host-name:28443/Administration” in an Internet browser window, where “host-name” is the host name of the IP Office Contact Center server.

Log in using the administrator credentials.



IP Office Contact Center Administration

User Name

Password

Language  ▼

Login

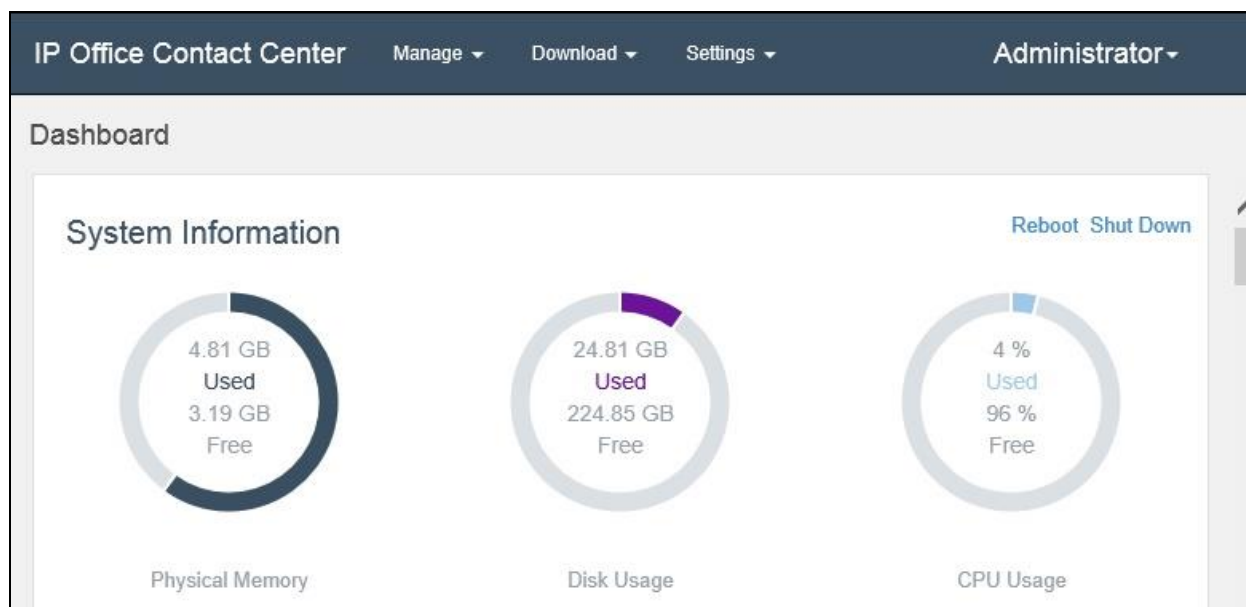
By logging in, you agree to be bound by the terms of the [End User License Agreement](#).

©2017 Avaya Inc. All Rights Reserved.

Best viewed in Internet Explorer 11, Google Chrome 39, or Mozilla Firefox 34 or greater

## 5.2. Verify License

The **Dashboard** screen is displayed. Select **Settings** → **License** from the top menu.



The **License Manager - Information** screen is displayed next. Scroll the screen as necessary, and verify that there is sufficient license for **Number of concurrent Team Leaders**, as shown below.

The screenshot shows the 'License Manager - Information' screen. It contains four input fields: 'WebLM Address' (10.64.101.235), 'Port Number' (52233), 'URN' (/WebLM/LicenseServer), and 'WebLM Client ID' (Client ID). Below these fields is a table with license information.

Feature	Expiration D...	Licensed	Acquired
Number of concurrent User with Extended Voice features	Permanent	10	3
Number of concurrent Team Leaders	Permanent	10	1
Number of concurrent Supervisors	Permanent	10	1
Number of IPOCC Wallboard	Permanent	10	0

### 5.3. Launch User Interface

From the IP Office Contact Center server, select **Start → Apps**, and click on **User Interface** to display the screen below. Log in using administrative credentials.



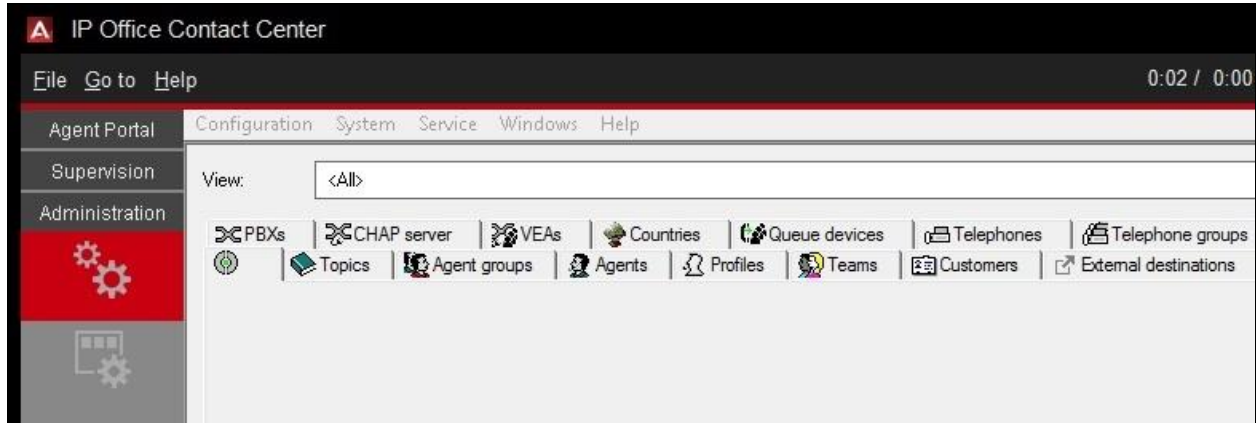
The image shows the Avaya IP Office Contact Center User Interface login screen. At the top, the Avaya logo is displayed in red. Below the logo, the text "IP Office Contact Center" is centered. The login form consists of three input fields on the left and two buttons on the right. The input fields are labeled "Username", "Password", and "Telephone Extension". The "Telephone Extension" field has a dropdown menu with "<None>" selected. The buttons are labeled "Login" and "Exit".

Username	<input type="text"/>	<input type="button" value="Login"/>
Password	<input type="password"/>	
Telephone Extension	<input type="text" value=" &lt;None&gt;"/>	<input type="button" value="Exit"/>

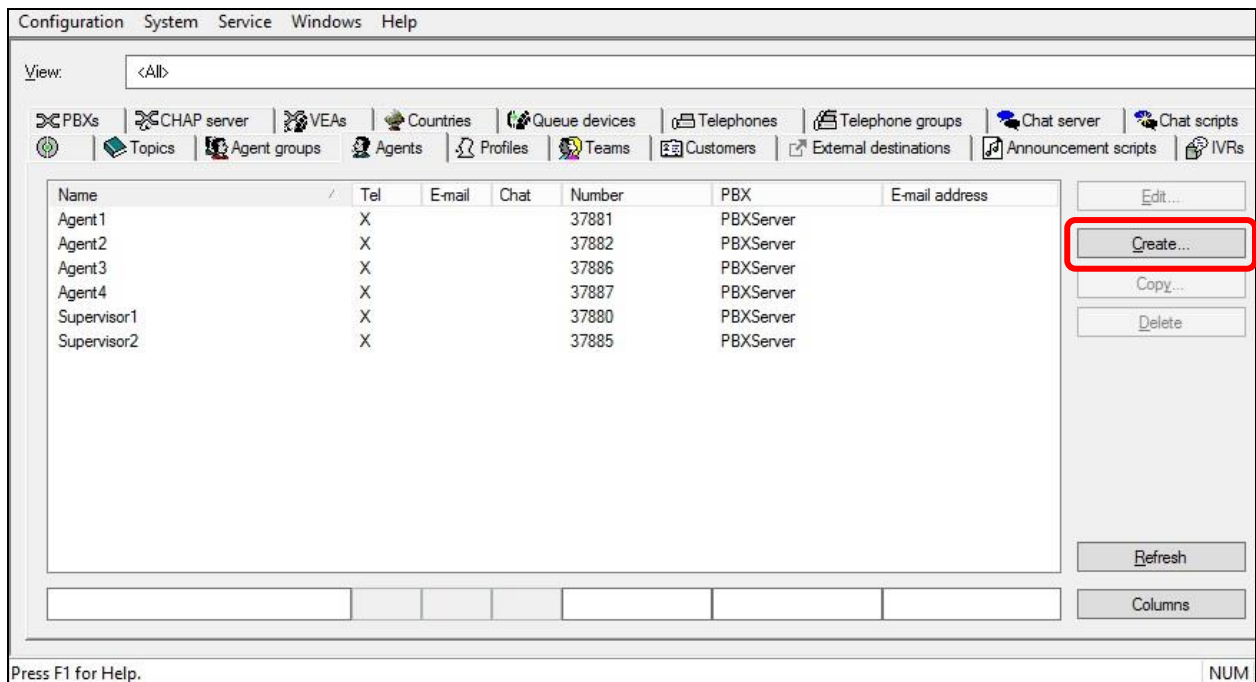


## 5.4. Administer Agents

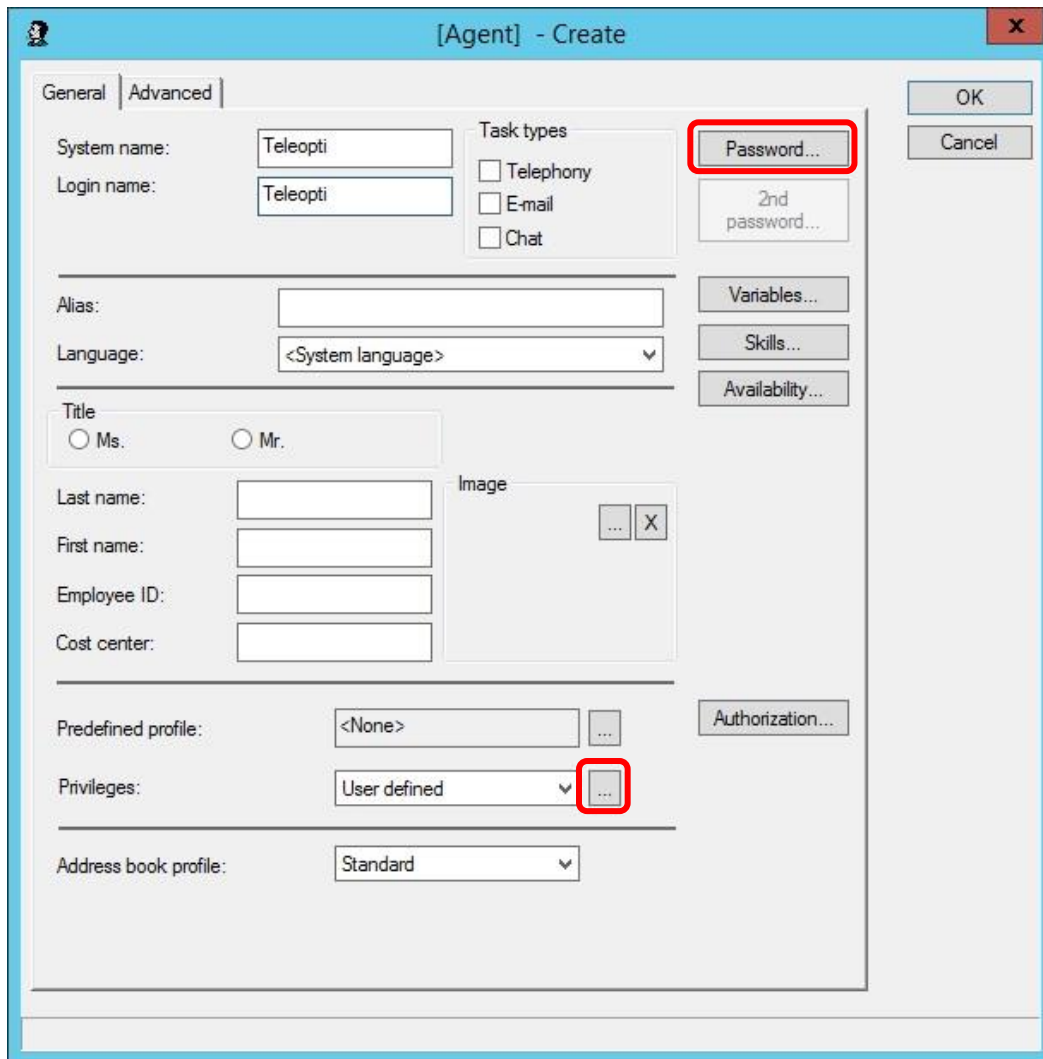
The **IP Office Contact Center** screen is displayed. Expand **Administration** in the left pane, and click on the **Settings** icon shown below.



Select the **Agents** tab, to display a list of agent users. Select **Create** to create a new agent user for WFM.

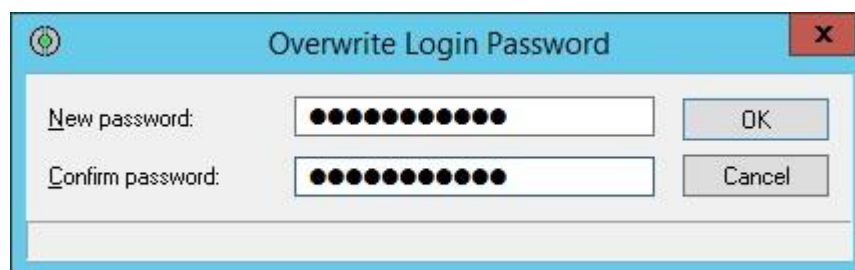


The **[Agent] – Create** screen is displayed. Enter desired **System name** and **Login name**, and retain the default values in the remaining fields. Select **Password**.



In the **Overwrite Login Password** pop-up box, enter desired password, and click **OK**.

The **[Agent] – Create** screen from above is displayed again. Click on the box next to **Privileges**.

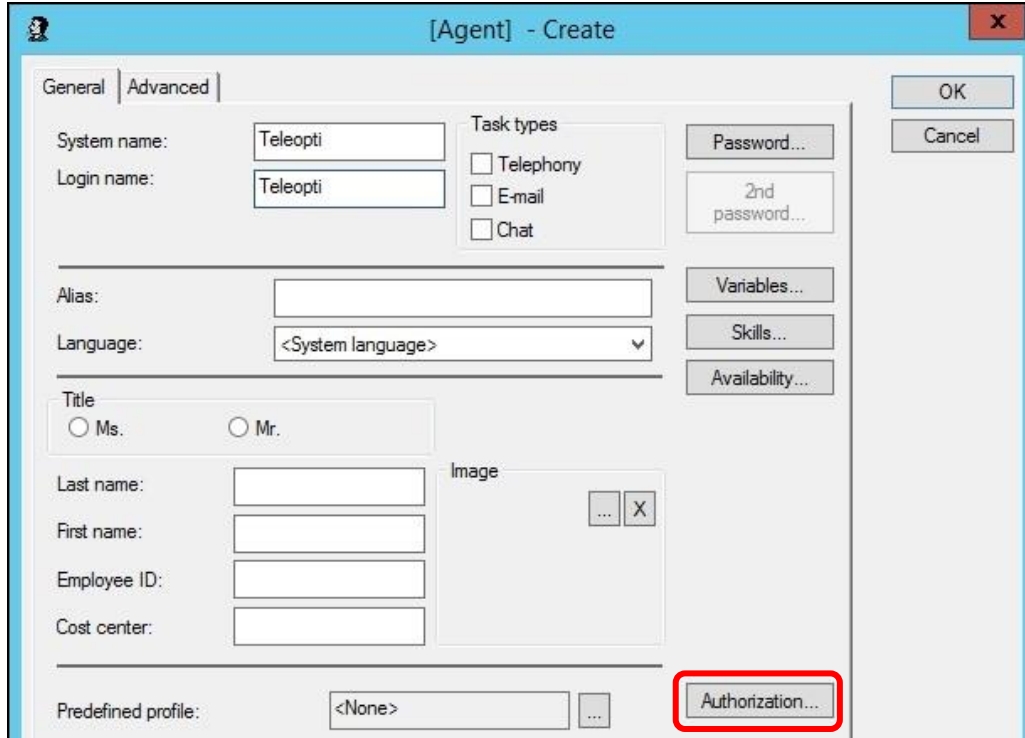


The **Agent privileges** screen is displayed. Check all parameters under **Team leader**, as shown below.

The image shows a dialog box titled "Agent privileges" with a close button (X) in the top right corner. The dialog has several tabs: Agent, UI, E-mail, Configuration, Variables, Reporting, Realtime Information, Task Flow Editor, and Others. The "Configuration" tab is currently selected. Inside the dialog, there are three main sections: Agent, Team leader, and Supervisor. Each section has a list of checkboxes and a "P" column. The "Team leader" section has three checkboxes checked: Realtime information, Remote functions, and Out of office notice. The "Supervisor" section has two checkboxes unchecked: Configuration and Silent Monitoring. The "Agent" section has four checkboxes unchecked: Callback from call list, Delete from call list, All agents (Authorization), and Pick up. The "Realtime Information" section has two checkboxes checked: Trunk realtime information and Agent History. The "Task Flow Editor" section has two checkboxes unchecked: Redirect and Redirect from Queue. The "Supervisor Emergency" and "Supervisor Assistance" checkboxes are also unchecked.

Section	Parameter	P
Agent	<input type="checkbox"/> Callback from call list	<input type="checkbox"/>
	<input type="checkbox"/> Delete from call list	<input type="checkbox"/>
	<input type="checkbox"/> All agents (Authorization)	<input type="checkbox"/>
	<input type="checkbox"/> Pick up	<input type="checkbox"/>
Team leader	<input checked="" type="checkbox"/> Realtime information	<input type="checkbox"/>
	<input checked="" type="checkbox"/> Remote functions	<input type="checkbox"/>
	<input checked="" type="checkbox"/> Out of office notice	<input type="checkbox"/>
Supervisor	<input type="checkbox"/> Configuration	<input type="checkbox"/>
	<input type="checkbox"/> Silent Monitoring	<input type="checkbox"/>
Realtime Information	<input checked="" type="checkbox"/> Trunk realtime information	<input type="checkbox"/>
	<input checked="" type="checkbox"/> Agent History	<input type="checkbox"/>
Task Flow Editor	<input type="checkbox"/> Redirect	<input type="checkbox"/>
	<input type="checkbox"/> Redirect from Queue	<input type="checkbox"/>
Supervisor	<input type="checkbox"/> Supervisor Emergency	<input type="checkbox"/>
	<input type="checkbox"/> Supervisor Assistance	<input type="checkbox"/>

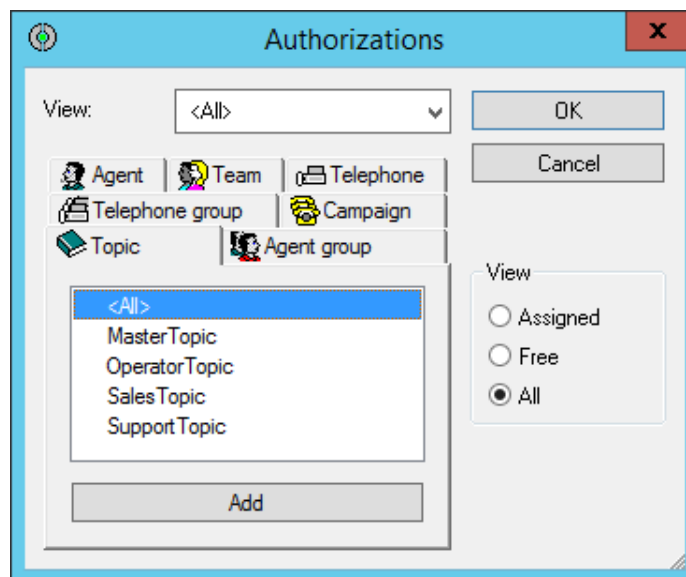
The **[Agent] – Create** screen is displayed again. Select **Authorization**.



The screenshot shows the "[Agent] - Create" dialog box with the "General" tab selected. The "System name" and "Login name" fields are both set to "Teleopti". The "Task types" section has checkboxes for "Telephony", "E-mail", and "Chat", all of which are unchecked. The "Alias" field is empty, and the "Language" dropdown is set to "<System language>". The "Title" section has radio buttons for "Ms." and "Mr.", both of which are unselected. The "Last name", "First name", "Employee ID", and "Cost center" fields are all empty. The "Image" section has a button with an ellipsis and an "X" button. The "Predefined profile" dropdown is set to "<None>". The "Authorization..." button is highlighted with a red rectangle. The "OK" and "Cancel" buttons are in the top right corner.

The **Authorizations** screen is displayed. Select the **Topic** tab. Select the desired topics to be monitored by WFM, followed by **Add**. In the compliance testing, the **<All>** entry was selected to enable WFM to monitor all topics.

Repeat this procedure to set the desired resources to be monitored by WFM in all remaining tabs. In the compliance testing, the **<All>** entry was selected in all tabs.

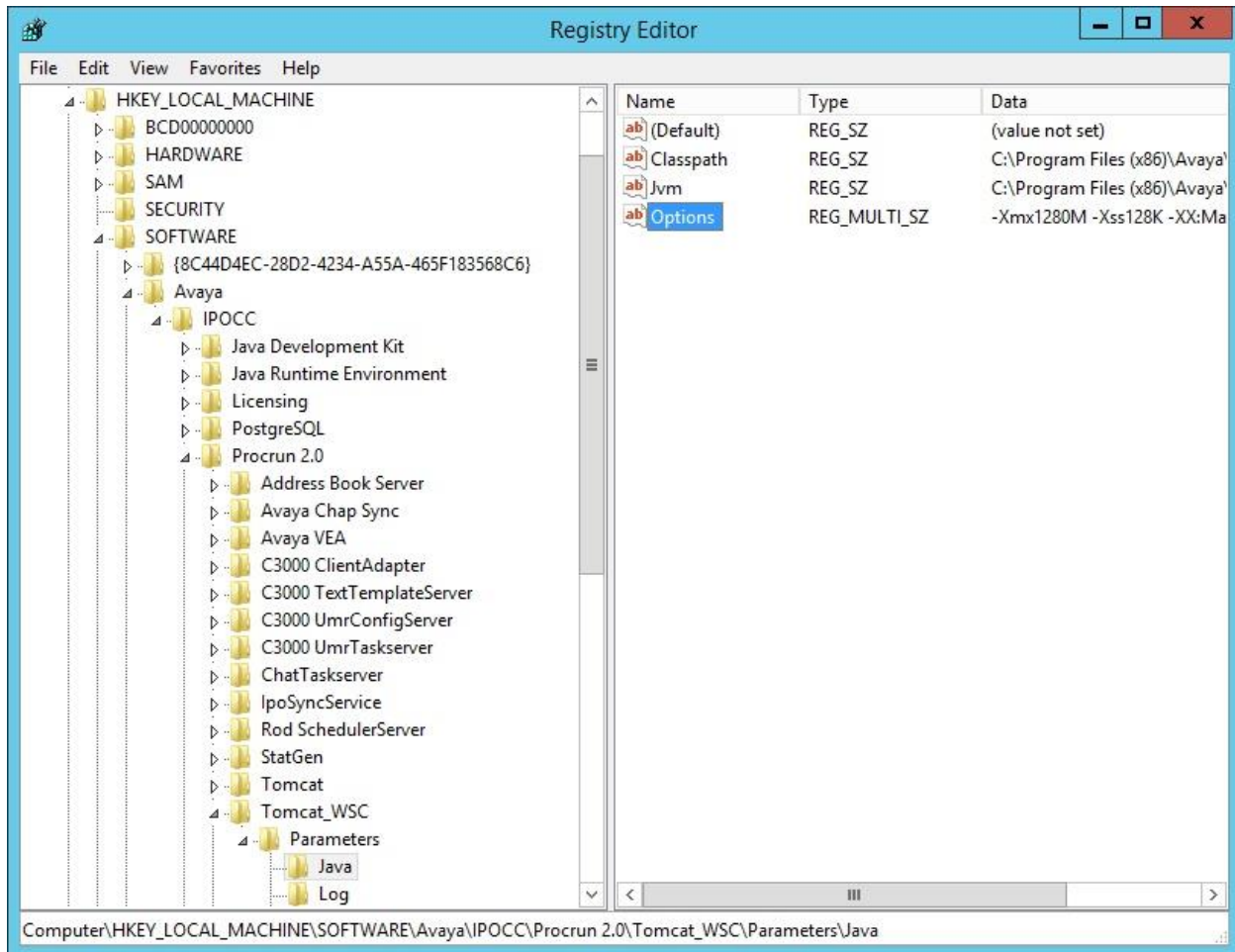


The screenshot shows the "Authorizations" dialog box with the "Topic" tab selected. The "View" dropdown is set to "<All>". The "Agent" tab is selected in the top left. The "Topic" list contains the following entries: "<All>", "MasterTopic", "OperatorTopic", "Sales Topic", and "Support Topic". The "<All>" entry is selected. The "Add" button is at the bottom. The "View" section on the right has radio buttons for "Assigned", "Free", and "All", with "All" selected. The "OK" and "Cancel" buttons are in the top right corner.

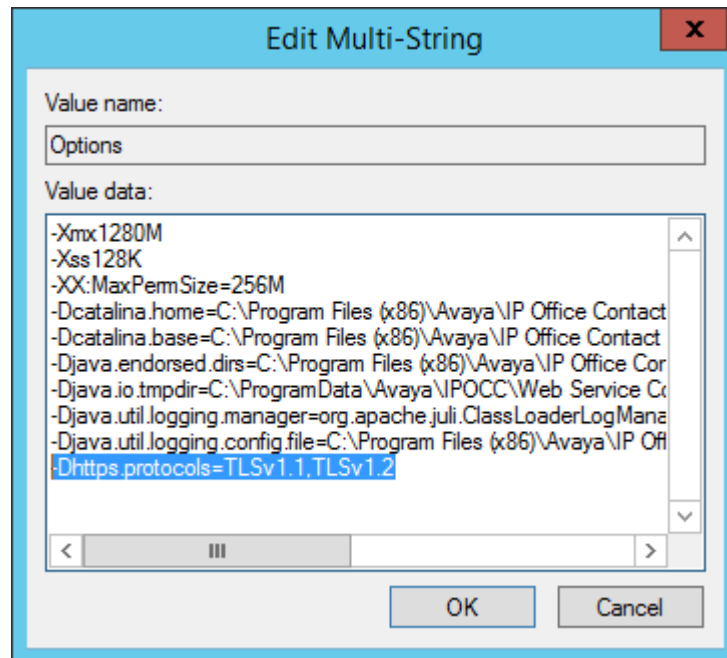
## 5.5. Administer Registry

For IP Office Contact Center servers that are upgraded from release 9.x, the registry setting needs to be updated to enable support for TLS 1.1 and 1.2.

Select **Start → Run**, and enter “regedit” to display the **Registry Editor** screen. Navigate to **Computer → HKEY\_LOCAL\_MACHINE → SOFTWARE → Avaya → IPOCC → Procrun 2.0 → Tomcat\_WSC → Parameters → Java**, and double click on the **Options** parameter shown below.

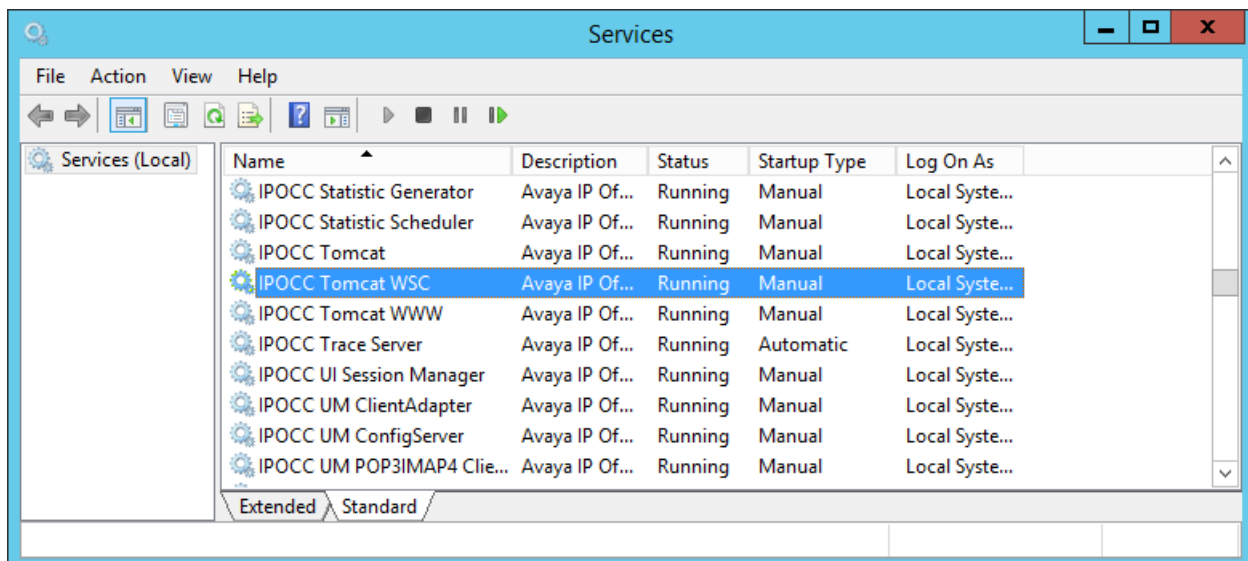


The **Edit Multi-String** dialog box is displayed. Add the “-Dhttps.protocols=TLSv1.1, TLSv1.2” line as shown below.



## 5.6. Start Services

Select **Start → Administrative Tools → Services** to display the **Services** screen. Restart the **IPOCC Tomcat WSC** service.



## 6. Configure Teleopti WFM

This section provides the procedures for configuring WFM. The procedures include the following areas:

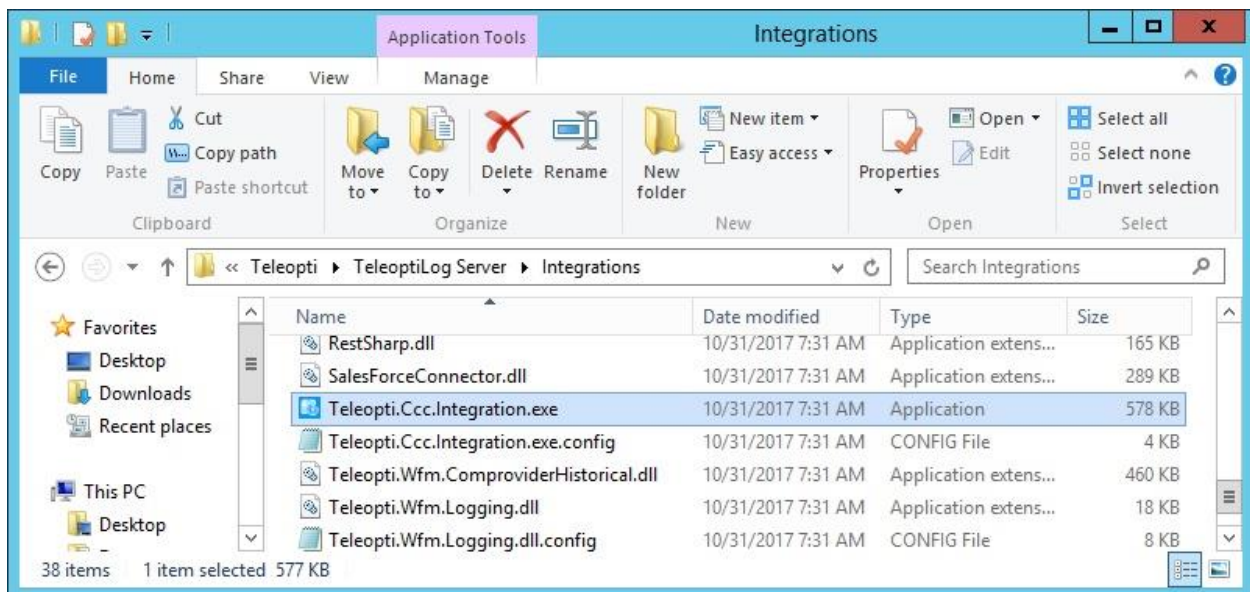
- Administer Teleopti WFM Integrations
- Administer agents
- Administer state groups and states
- Administer people

The configuration of WFM is typically performed by Teleopti Professional Services. The procedural steps are presented in these Application Notes for informational purposes.

The Certificate Authority root certificate and the WFM server identity certificate are assumed to be pre-installed on the WFM server.

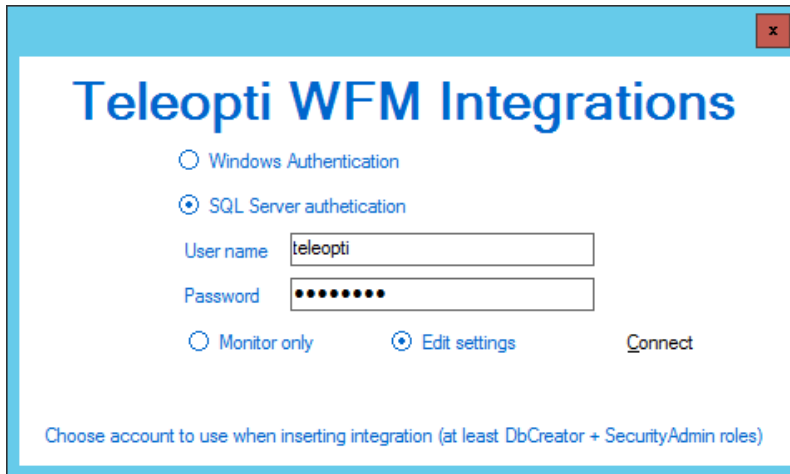
### 6.1. Administer Teleopti WFM Integrations

From the WFM server running the Log Server component, navigate to the **C:\Program Files (x86)\Teleopti\TeleoptiLog Server\ Integrations** directory, and double click on **Teleopti.Ccc.Integration.exe**.





The **Teleopti WFM Integrations** screen is displayed. Retain the default values and click **Connect**.



The image shows a dialog box titled "Teleopti WFM Integrations". It has two radio buttons: "Windows Authentication" (unselected) and "SQL Server authentication" (selected). Below these are two text boxes: "User name" containing "teleopti" and "Password" containing eight dots. At the bottom, there are two radio buttons: "Monitor only" (unselected) and "Edit settings" (selected), followed by a "Connect" button. A note at the bottom states: "Choose account to use when inserting integration (at least DbCreator + SecurityAdmin roles)".

The screen below is displayed next. Select and expand the pertinent and pre-configured aggregation database in the left pane, followed by **RTA** under the relevant logging object, in this case **TeleoptiAgg\_IPOCC → IPOCC → RTA**. This **Source** screen is displayed. Enter the following values for the specified fields.

- **AccessLoginName:** The agent user credentials from **Section 5.4**.
- **AccessPassword:** The agent user credentials from **Section 5.4**.
- **DirectoryWsHost:** The IP address of the IP Office Contact Center server.
- **DirectoryWsPort:** "18443"
- **MonitoringWsEndpointObser:** "5443"
- **MonitoringWsHost:** The IP address of the IP Office Contact Center server.
- **MonitoringWsPort:** "18443"
- **UseIpAddressForMonitorObs:** "YES"
- **UseSSL:** "True"



The image shows a window titled "Teleopti WFM Integrations - Data Import Configuration Tool - Version 7.2.1.74979". On the left is a tree view with "Monitor" expanded, showing "TeleoptiAgg\_Demo", "TeleoptiAgg\_IPOCC", and "(1) IPOCC" expanded to show "RTA", "Stats Import", and "File Import". The "RTA" node is selected. The main area is titled "Source" and contains a list of fields with corresponding values in text boxes:

AccessLoginName	Teleopti
AccessPassword	*****
DirectoryWsHost	10.64.101.227
DirectoryWsPort	18443
MonitoringWsEndpointObser	5443
MonitoringWsHost	10.64.101.227
MonitoringWsPort	18443
UseIpAddressForMonitorObs	<input checked="" type="checkbox"/> YES
UseSSL	True



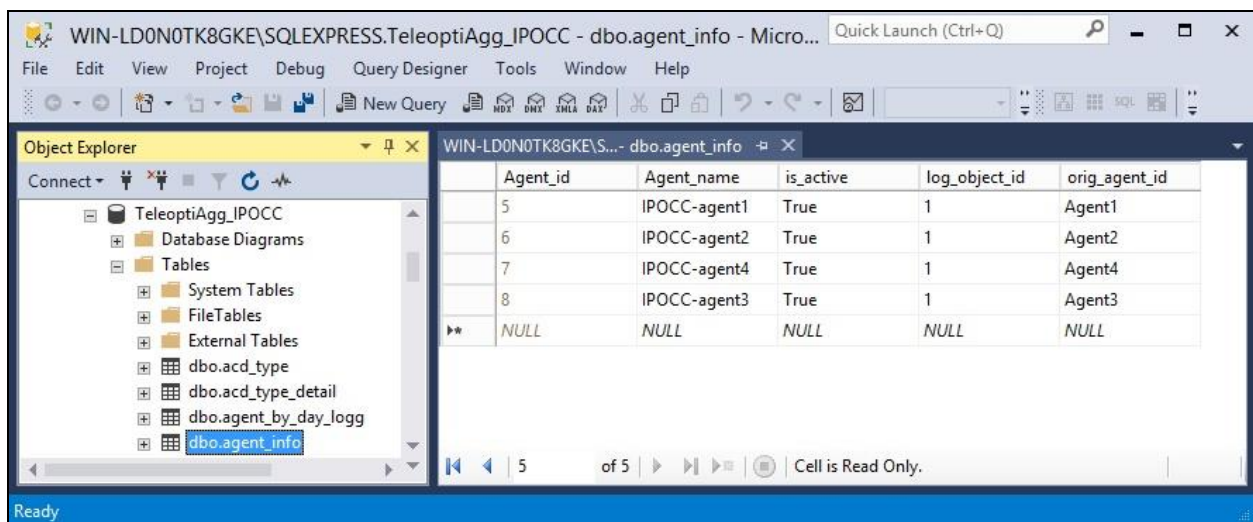
## 6.2. Administer Agents

From the WFM server running the SQL Server component, navigate to **Start → Apps → Microsoft SQL Server Management Studio 17** to launch and connect to the SQL Server.



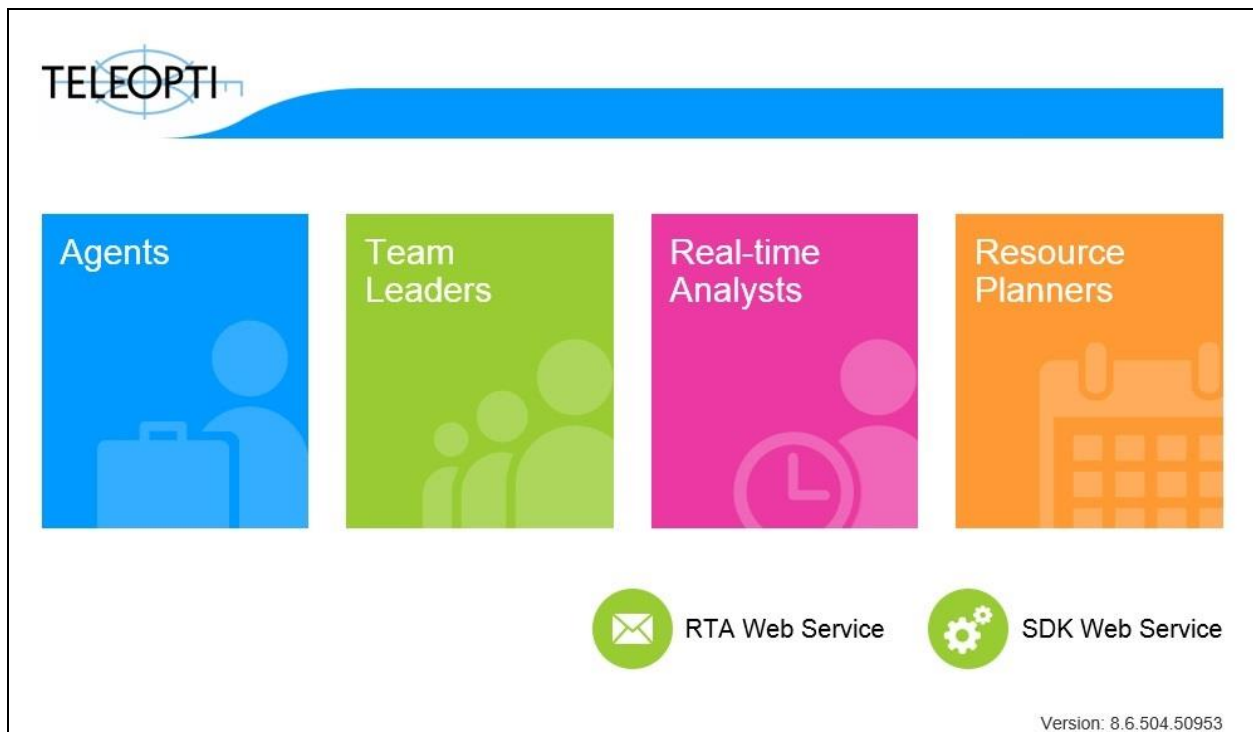
Expand the relevant database tables, in this case **TeleoptiAgg\_IPOCC → Tables**. Right click on the **dbo.agent\_info** entry and select **Edit Top 200 Rows**. In the right pane, add an entry for each agent to monitor from **Section 5.4**.

- **Agent\_name:** A desired and unique name.
- **is\_active:** “True”
- **log\_object\_id:** The relevant object ID, in this case “1”.
- **orig\_agent\_id:** The corresponding agent name from **Section 5.4**.

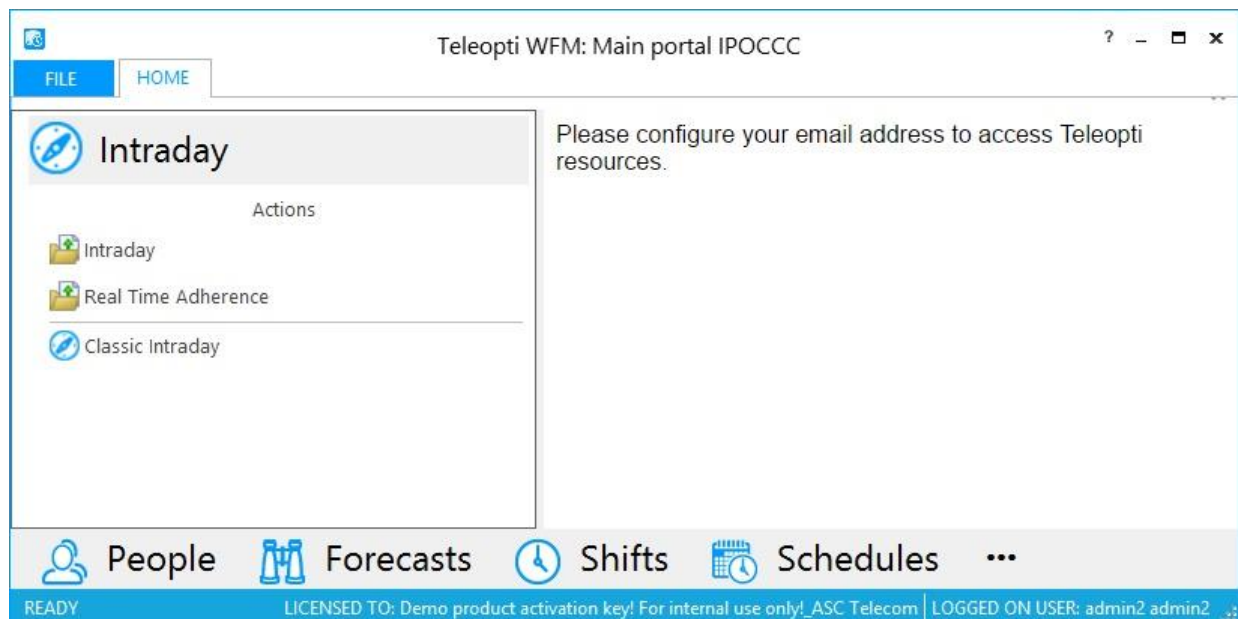


### 6.3. Administer State Groups and States

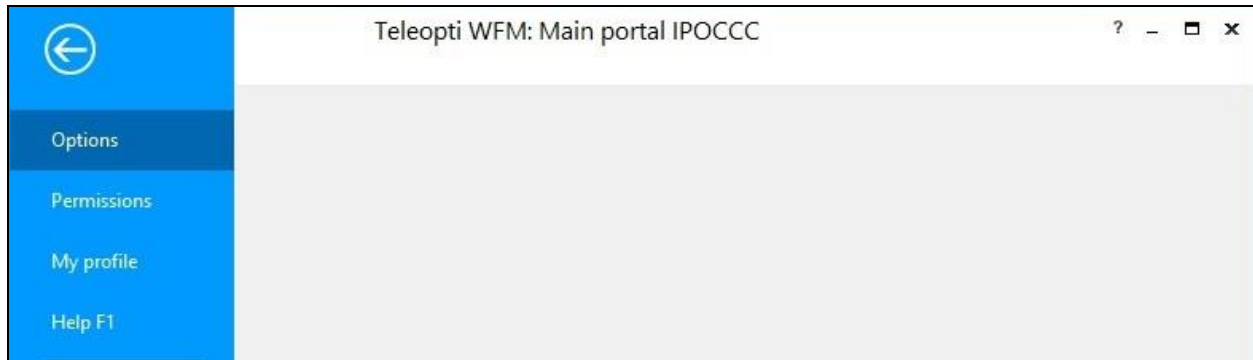
From the WFM server, access the web interface by using the URL “http://host-name/TeleoptiWFM” in an Internet browser window, where “host-name” is the host name of the WFM server running the Web component. Log in using the administrative credentials (not shown). The **TELEOPTI** screen below is displayed. Select **Resource Planners**.



The **Teleopti WFM: Main portal IPOCCC** screen is displayed next. Select the **FILE** tab.

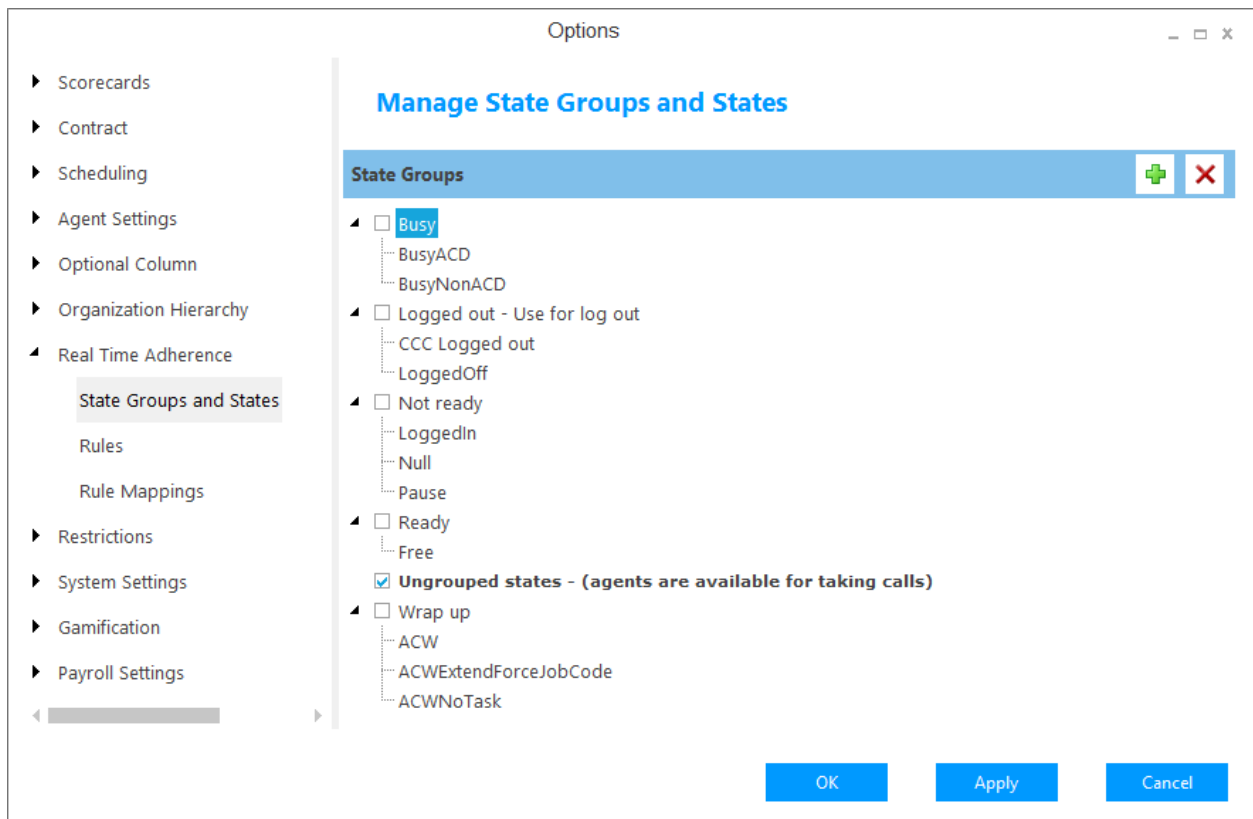


The screen is updated as shown below. Select **Options** in the left pane.



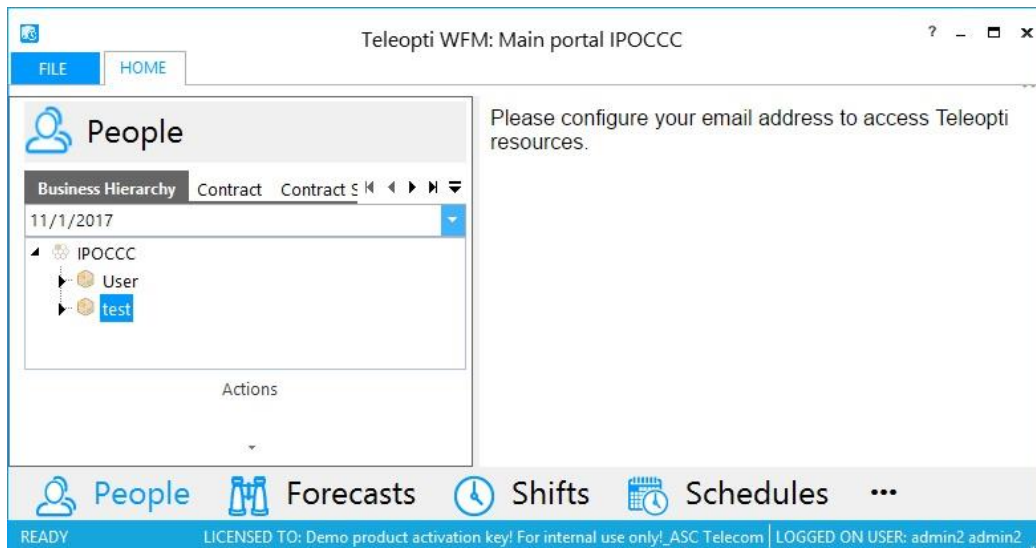
In the updated screen, select **Real Time Adherence → State Groups and States** in the left pane, to display the **Manage State Groups and States** screen.

The **Manage State Groups and States** screen will be initially empty, with only the **Ungrouped states** category. As new agent states are received from IP Office Contact Center, the states will begin to appear in this screen and shown under the **Ungrouped states** category. Follow reference [4] to create desired groups and drag the ungrouped states into the created groups. The screen below shows the states groups and states generated and configured in the compliance testing.



## 6.4. Administer People

Follow the procedures in **Section 6.3** to display the **Teleopti WFM: Main portal IPOCCC** screen. Select **People** from the bottom of the screen, followed by the **Business Hierarchy** tab in the left pane. Double click on the pre-configured site entry, in this case “test”.



The **People – Teleopti WFM** screen is displayed next. Follow reference [4] to create an entry for each agent from **Section 6.2**. Note that the available external logons shown in the right pane were automatically picked up from IP Office Contact Center via the WSC interface.

- **Full name:** A desired and unique name.
- **Site/Team:** Select the pertinent pre-configured site and team, in this case “test/test”.
- **External logon:** Select the pertinent logon name from the right pane, as shown below.

	Full name	Date	Site/Team	Skills	External logon
1	Agent1 Primary	10/16/2017	test/test		IPOCC-agent1 (IPOCC)
2	Agent2 Primary	10/16/2017	test/test		IPOCC-agent2 (IPOCC)
3	Agent3 Expansion	10/16/2017	test/test		IPOCC-agent3 (IPOCC)
4	Agent4 Expansion	10/16/2017	test/test		IPOCC-agent4 (IPOCC)

Has	External logon	Log object
<input checked="" type="checkbox"/>	IPOCC-agent1	IPOCC
<input type="checkbox"/>	IPOCC-agent2	IPOCC
<input type="checkbox"/>	IPOCC-agent3	IPOCC
<input type="checkbox"/>	IPOCC-agent4	IPOCC

## 7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of IP Office Contact Center and WFM.

Access the WFM web interface by using the URL “http://ip-address/TeleoptiWFM” in an Internet browser window, where “ip-address” is the IP address of the WFM server hosting the Web component. Log in using the appropriate credentials (not shown).

The **Teleopti WFM IPOCCC** screen is displayed. Select **Real Time Adherence** from the left pane, to display a list of monitored agents and their states. Verify that all agent states are reflected properly.

Teleopti WFM IPOCCC

Agents DASHBOARD AGENTS

Monitor up to 50 agents

Select a skill Select skill area Teams: test

Filter agent na

IN ALARM ALL

Name ↑	Site/Team	18:00	19:00	20:00	21:00	State
Agent1 Primary	test/test					Not ready
Agent2 Primary	test/test					Logged out
Agent3 Expansion	test/test					Logged out
Agent4 Expansion	test/test					Ready

Establish an ACD call from the PSTN with an IP Office Contact Center agent. Verify that the answering agent's state is updated properly, in this case "Agent4 Expansion" state updated to "Busy", as shown below.

The screenshot displays the Teleopti WFM IPOCCC interface. The left sidebar contains navigation links: Permissions, Requests, Real Time Adherence (highlighted), Intraday, Teams, Reports, and MyTime. The main content area is titled 'Agents' and includes a 'DASHBOARD' button and an 'AGENTS' button. Below these, it says 'Monitor up to 50 agents'. There are input fields for 'Select a skill', 'Select skill area', and 'Teams: test'. A filter section shows 'Filter agent na' and buttons for 'IN ALARM' and 'ALL'. The main table lists agents with columns for Name, Site/Team, and time slots (18:00, 19:00, 20:00, 21:00). The 'State' column shows the current status of each agent.

Name ↑	Site/Team	18:00	19:00	20:00	21:00	State
Agent1 Primary	test/test					Not ready
Agent2 Primary	test/test					Logged out
Agent3 Expansion	test/test					Logged out
Agent4 Expansion	test/test					Busy

## 8. Conclusion

These Application Notes describe the configuration steps required for Teleopti WFM to successfully interoperate with Avaya IP Office Contact Center. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

## 9. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Using Avaya IP Office Contact Center Web Administration Portal*, Release 10.1, Issue 1, May 2017, available at <http://support.avaya.com>.
2. *Using the Avaya IP Office Contact Center Configuration and User Interface Configuration Modules*, Release 10.1, Issue 1, May 2017, available at <http://support.avaya.com>.
3. *Administering Avaya IP Office™ Platform with Manager*, Release 10.1, June 2017, available at <http://support.avaya.com>.
4. *Teleopti WFM Installation Guide*, 2017-06-02, available at <http://www.teleopti.com>.

---

**©2017 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).