A MITEL
PRODUCT
GUIDE

Mitel OpenScape Contact Center Enterprise V12

System Management Guide V12

System Management Guide

Service Documentation
10/2024

A31003-S22C0-S101-01-7620

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

1 About this guide . . . 7
1.1 Who should use this guide . . . 7
1.2 Formatting conventions . . . 7
1.3 Documentation feedback . . . 8
2 Configuring a wallboard . . . 9
2.1 Before you begin . . . 9
2.2 Configuring the IP connection for a wallboard . . . 9
3 Configuring the corporate e-mail server . . . 11
3.1 Corporate e-mail server requirements . . . 11
3.2 Planning the Microsoft Office 365 deployment . . . 12
3.3 Planning the Google GSuite deployment . . . 13
3.4 Planning the Microsoft Exchange deployment . . . 14
3.4.1 Specifying custom headers (Microsoft Exchange Server 2007, 2010, and 2013 only) . . . 15
3.5 Planning the IBM Lotus Domino deployment . . . 16
3.5.1 Compacting the database . . . 17
3.6 Setting up a secure connection for an e-mail server . . . 18
3.7 Using authentication on an e-mail server . . . 19
3.8 Supporting the e-mail reports feature . . . 19
4 Configuring the corporate Web server . . . 21
4.1 System requirements for using Web components . . . 21
4.1.1 Corporate Web server requirements . . . 21
4.1.2 Web browser requirements . . . 21
4.2 Configuring Web components . . . 22
4.2.1 Configuring an IIS server . . . 22
4.2.1.1 Configuring the Web component files on an IIS server . . . 23
4.2.1.2 Testing Web collaboration on an IIS server . . . 25
4.2.1.3 Testing Web callback on an IIS server . . . 26
4.2.1.4 Testing VoiceXML integration on an IIS server . . . 26
4.2.2 Configuring a Tomcat server . . . 27
4.2.2.1 Configuring the .war file on a Tomcat server . . . 27
4.2.2.2 Testing Web collaboration on a Tomcat server . . . 29
4.2.2.3 Testing Web callback on a Tomcat server . . . 30
4.2.2.4 Testing VoiceXML integration on a Tomcat server . . . 30
4.2.3 Configuring a Sun Java System Web Server . . . 31
4.2.3.1 Configuring the .war file on a Sun Java System Web Server . . . 31
4.2.3.2 Testing Web collaboration on a Sun Java System Web Server . . . 33
4.2.3.3 Testing Web callback on a Sun Java System Web Server . . . 34
4.3 Setting up a secure connection for a Web server . . . 34
4.3.1 Enabling TLS on an IIS server . . . 35
4.3.2 Enabling TLS on a Tomcat or Sun Java server . . . 36
4.4 Localizing and customizing Web components . . . 37
4.4.1 Localizing Web components . . . 37
4.4.2 Customizing Web components . . . 38
4.5 Troubleshooting Web collaboration . . . 40
4.5.1 Web server configuration issues . . . 40
4.5.2 General connection issues . . . 40

4.6 Web callback error codes . . . 42

5 Configuring the presence integration . . . 43
5.1 Configuring an OpenScape UC Application user account . . . 43
5.2 Configuring the external LDAP directory . . . 44

6 Maintaining the system . . . 45
6.1 Shutting down a server machine for system maintenance . . . 45
6.2 Changing the OpenScape Contact Center and Informix passwords . . . 46
6.3 Backing up the database . . . 48
6.3.1 Scheduling a database backup . . . 49
6.3.2 Backing up the database using the ontape utility . . . 50
6.3.2.1 Backing up the database to a local tape drive . . . 50
6.3.2.2 Backing up the database to a local or network drive . . . 51
6.3.3 Restoring the database using the ontape utility . . . 52
6.3.4 Restoring a zero level backup made using ontape utility . . . 53
6.3.5 Backing up the database using the onbar utility . . . 54
6.3.6 Restoring the database using the onbar utility . . . 55
6.4 SNMP support . . . 55
6.4.1 OpenScape Contact Center SNMP extension agent . . . 56
6.4.2 OpenScape CAP Fault Management software . . . 57

7 Managing a central reporting environment . . . 59
7.1 Managing replication for central reporting . . . 59
7.1.1 About the replication buffer . . . 59
7.1.2 Suspending replication for central reporting . . . 60
7.1.2.1 Resuming central reporting replication . . . 62
7.1.3 Shutting down all replication for central reporting . . . 63
7.1.3.1 Restarting central reporting replication . . . 65
7.2 Synchronizing the reporting data for central reporting . . . 66
7.3 Troubleshooting the replication configuration for central reporting . . . 68
7.4 Replacing a main server machine for central reporting . . . 71
7.4.1 Reconfiguring the replication settings . . . 71

8 Managing a high availability (warm standby) environment . . . 73
8.1 Managing replication for high availability (warm standby) . . . 73
8.1.1 Suspending high availability (warm standby) replication . . . 73
8.1.1.1 Resuming high availability (warm standby) replication . . . 75
8.1.2 Suspending central reporting replication . . . 76
8.1.2.1 Resuming central reporting replication . . . 76
8.1.3 Stopping high availability (warm standby) replication . . . 76
8.1.3.1 Restarting high availability (warm standby) replication . . . 77
8.1.4 Stopping central reporting replication . . . 79
8.1.4.1 Restarting central reporting replication . . . 80
8.1.5 Shutting down all replication . . . 83
8.1.5.1 Restarting all replication . . . 84
8.2 Synchronizing the data between the primary and backup server machines . . . 85
8.3 Synchronizing the administration data between the primary and central reporting server machines . . . 87
8.4 Synchronizing the reporting data for high availability (warm standby) with central reporting . . . 88
8.5 Troubleshooting the replication configuration for high availability (warm standby) . . . 91
8.6 Restoring the database . . . 91
8.6.1 Restoring the database on the server machine that is in standby mode . . . 91
8.6.2 Restoring the database on the central reporting server machine . . . 92
8.6.3 Restoring the database on more than one server machine . . . 93

8.7 Forcing a single server machine into service 94
8.8 Replacing a server machine in the cluster 95

9 Microsoft Teams deployment 97
9.1 Editing the tab URL manually 97
9.2 Uploading to Microsoft Teams 97

10 Exchange Calendar Integration 99
10.1 Azure Configuration 99

Index 106

1 About this guide

This guide describes how to configure third-party hardware, such as wallboards, corporate e-mail servers, and corporate Web servers, to integrate with the Unify OpenScape Contact Center Enterprise V12 system. It also describes how to perform ongoing maintenance of the Unify OpenScape Contact Center Enterprise V12 system, including backing up and restoring the database.

1.1 Who should use this guide

This guide is intended for users within the organization who are responsible for managing, monitoring, and maintaining the health of the Unify OpenScape Contact Center Enterprise V12 system.

1.2 Formatting conventions

The following formatting conventions are used in this guide:

Bold
This font identifies Unify OpenScape Contact Center Enterprise V12 components, window and dialog box titles, and item names.

Italic
This font identifies references to related documentation.

`Monospace Font`
This font distinguishes text that you should type, or that the computer displays in a message.

NOTE: Notes emphasize information that is useful but not essential, such as tips or alternative methods for performing a task.

IMPORTANT: Important notes draw special attention to actions that could adversely affect the operation of the application or result in a loss of data.

1.3 Documentation feedback

To report an issue with this document, call the Customer Support Center.

When you call, be sure to include the following information. This will help identify which document you are having issues with.

- **Title:** System Management Guide
- **Order Number:** A31003-S22C0-S101-01-7620

2 Configuring a wallboard

This chapter describes how to configure a wallboard. A wallboard is an electronic message board that displays a scrolling view of real-time statistical data and general system information about the contact center to several users at once. The OpenScape Contact Center system supports Spectrum IP Wallboards, version 4200 R, as well as custom wallboards that adhere to the EZ Key II protocol.

IMPORTANT: Only properly trained personnel should configure a wallboard. Attempts to configure a wallboard by personnel who are not properly trained may adversely affect the operation of the OpenScape Contact Center system.

2.1 Before you begin

Before you can install and configure the wallboard, you must do the following:

- If you have a Spectrum Serial Wallboard, you must obtain a serial-to-IP conversion kit (NIU in North America and UDS100 in the International Market).
- Obtain a static IP address for the wallboard.
- Ensure that you have the supported firmware versions that are compliant with the OpenScape Contact Center system.

2.2 Configuring the IP connection for a wallboard

This procedure describes how to configure the IP connection for a wallboard. It assumes that you have already installed the Lantronix Device Server Configuration Utility 2.0 software for the wallboard on the OpenScape Contact Center main server machine.

IMPORTANT: Only basic configuration steps are provided. For detailed instructions and precautions, refer to the vendor’s documentation.

To configure the IP connection for a wallboard:

1. Connect the wallboard to the Local Area Network (LAN).
2. Start the Lantronix Device Server Configuration Utility application.
3. On the **File** menu, click **Search Network**.
4. To search the network for an existing wallboard, do the following:
   a) Click **Start Search**.
   b) When the wallboard devices have been successfully located on the network, click **Save**.
   c) When the system informs you that the devices have been saved, click **OK**.
   d) Click **Back**.
5. Select the IP address of the wallboard you want to configure.
6. On the **Tools** menu, click **Device Manager**.
7. Click **Web Configuration**.
8. Click **OK**. This launches the Lantronix Web-Manager.
9. Under **Dedicated Connection**, type the wallboard's port number in the **Local Port** box, and then click **Update Settings**.

NOTE: To configure a new board that does not already have an IP address, on the **Tools** menu, click **Assign IP Address**. Locate the hardware or Ethernet address on the back of the wallboard, and then type it in the provided field. Assign the wallboard an IP address, and then click **Set IP Address**.

---

3 Configuring the corporate e-mail server

This chapter describes how to configure the corporate e-mail server to support the OpenScape Contact Center e-mail feature and the e-mailing of reports. E-mail messages sent by customers are routed through the corporate e-mail server to the OpenScape Contact Center E-mail Server. All e-mail messages are stored in a single mailbox on the corporate e-mail server.

The OpenScape Contact Center E-mail Server and the corporate e-mail server communicate using the IMAP4 protocol. The OpenScape Contact Center client applications and the corporate e-mail server also use the IMAP4 protocol to retrieve and process e-mail messages. Message attachments are retrieved using separate IMAP4 and MIME functions. Reply e-mail messages are sent to customers from the E-mail Server using an SMTP interface.

NOTE: In the Manager application, the main corporate server is used to send reports for supervisors and for the keep-alive process.

3.1 Corporate e-mail server requirements

The following e-mail servers have been tested in conjunction with the OpenScape Contact Center system:

- Microsoft Office 365
- Microsoft Exchange Server 2016 and 2019
- Google GSuite

For more information on these servers, refer to the manufacturer’s documentation.

NOTE: We recommend that you safeguard the content on the corporate e-mail server to reduce the possibility of e-mail messages being inadvertently deleted.

Ensure that the corporate e-mail server is configured as follows:

- **NTLM authentication -** Ensure that the Corporate Email Server supports NTLM authentication

- **Client access licenses** – Ensure that you have sufficient client access licenses. Each user that is able to access the OpenScape Contact Center E-mail Server requires a client access license.
- **Custom headers** – The OpenScape Contact Center e-mail functionality uses custom headers, so you must ensure that the corporate e-mail server does not filter or remove custom headers from e-mail messages.
- **IMAP sessions** - One IMAP session is required for each day that has active messages associated with it. Each user requires an IMAP session when sending an email message or retrieving the contents of an email message.
- **Simultaneous connections** – Ensure that the OpenScape Contact Center e-mail account has been configured with a sufficient number of connections to support the number of users who will be accessing the account simultaneously.
- **Spam filtering and e-mail address blocking** – This stops unwanted e-mail messages from being routed to users.
- **Virus checking software** – Incoming e-mail messages and attachments from the corporate e-mail server must be checked for viruses.

3.2 Planning the Microsoft Office 365 deployment

You must carefully plan the Microsoft Office 365 deployment. When configuring the message retention period in the OpenScape Contact Center E-mail Server, be sure to take the Microsoft Office 365 database availability into consideration. For more information on this and other tasks described in this section, the contract to Microsoft Office 365 must be evaluated.

You must configure the following:

- **User accounts** - Create a new user account to be used by the OpenScape Contact Center E-mail Server. You must specify a password for the new user account.
- **Throttling policy** - Microsoft Office 365 has a throttling policy that limits the SMTP message rate to a maximum of 30 messages / minute. In order to comply with this limitation the OSCC parameter Message Rate Limit in E-mail Settings must be set to 30 (or less).

- **IMAP Sessions** - Microsoft Office 365 limits the number of active IMAP sessions to 20 sessions per account. In order to operate according to this limitation the OSCC parameter Maximum IMAP Sessions in E-mail Settings must be set to 20, from which 5 sessions are reserved for the OSCC Email server.

IMPORTANT: When the Contact Center schedule opens, the Routing Server starts distributing e-mails to the available agents. The distribution depends on the number of configured IMAP sessions. A throttling mechanism distributes the e-mails to the available agents. For example, there are 200 e-mails to be distributed to 100 available agents. Since 15 IMAP sessions are available, OSCC routes a maximum of 15 e-mails to agents and it waits up to 15 seconds before sending the next queued email messages to the next available agents. If a Client Desktop / Agent Portal is not able to establish an IMAP session, it waits for a random time and tries again. The Client Desktop / Agent Portal will try five times to establish the IMAP session to download e-mails before being switched to routing state *Unavailable*.

3.3 Planning the Google GSuite deployment

You must carefully plan the Google GSuite deployment. When configuring the message retention period in the OpenScape Contact Center E-mail Server, be sure to take the Google GSuite database availability into consideration. For more information on this and other tasks described in this section, the contract to Google GSuite must be evaluated.

You must perform the following configurations:

In Google GSuite:

- Create a new GMail user account to be used by the OpenScape Contact Center E-mail Server.
- In the Gmail settings, at the Forwarding and POP/IMAP tab, ensure "IMAP access" is enabled.
- In the Google Account security settings:
  - create an “application password” and use it in OpenScape Contact Center.
  - enable the option “allow less secure applications”

In OpenScape Contact Center:

- **IMAP Sessions** - Google GSuite limits the number of active IMAP sessions to 15 sessions per account. To operate according to this limitation the OSCC parameter **Maximum IMAP Sessions in E-mail Settings** must be set to 15, from which 5 sessions are reserved for the OSCC Email server.

3.4 Planning the Microsoft Exchange deployment

You must carefully plan the Microsoft Exchange deployment. When configuring the message retention period in the OpenScape Contact Center E-mail Server, be sure to take the Microsoft Exchange database size into consideration. For more information on this and other tasks described in this section, see the Microsoft Exchange documentation.

IMPORTANT: The Microsoft Exchange configuration should only be completed by a trained Microsoft Exchange Administrator.

You must configure the following:

- **User accounts** – Create a new user account to be used by the OpenScape Contact Center E-mail Server. You must specify a password for the new user account.
- **Aliases (optional)** – If required, configure additional SMTP e-mail addresses to be used as aliases for the new user account.

  If you want to present multiple contact e-mail addresses to your customers, you need to configure an alias for each additional e-mail address that points to the new user account. Creating an alias ensures that e-mail messages sent to the corporate e-mail server are routed to the OpenScape Contact Center E-mail Server mailbox for agent handling. For more information, see the *Manager Help*.

  Since Microsoft Exchange Server 2007 converts aliases to the main user account address for both internally and externally originating messages, you must configure an Exchange mailbox for each alias you want to use, and have the mailbox forward messages to the main user account. This is particularly important in a multitenant environment where it ensures that if a customer sends an e-mail message to an alias, such as sales@company1.com, it is routed to the appropriate business unit.It also ensures that the incoming e-mail address is not converted to the main account address on reply.
- **Throttling policy (Microsoft Exchange Server 2013)** – When using Microsoft Exchange Server 2013, the ImapMaxBurst and ImapRechargeRate values in the throttling policy can adversely

impact the e-mail throughput of the OpenScape Contact Center email account. To reach maximum throughput, we recommend that you create a specific throttling policy for the OpenScape Contact Center email account and set the ImapMaxBurst and ImapRechargeRate values to 8000000 or higher.

- **Shadow redundancy (Microsoft Exchange Server 2013)** – When using Microsoft Exchange Server 2013, the Shadow Redundancy feature in the transport configuration settings can adversely impact the e-mail throughput of the OpenScape Contact Center email account. To reach maximum throughput, we recommend that you set the ShadowRedundancyEnabled flag to false.

3.4.1 Specifying custom headers (Microsoft Exchange Server 2007, 2010, and 2013 only)

In Microsoft Exchange Server 2007, 2010, and 2013, custom headers that are required by the OpenScape Contact Center e-mail functionality might not be available through the Microsoft Exchange IMAP interface. If you want to use Microsoft Exchange Server 2007, 2010, or 2013 as your corporate IMAP e-mail server, you must run a utility program (osccmseheaders.exe) which sends a special e-mail message using the Microsoft Exchange SMTP interface. After the special e-mail message has been sent, the required custom headers will be available via the Microsoft Exchange IMAP interface.

Before you run the utility program, you must do the following:

- Configure Microsoft Exchange Server to support authenticated SMTP. The utility uses an authenticated SMTP session to specify the custom headers. If required, you can turn off authenticated SMTP after the utility has been successfully run.
- If you are using Microsoft Exchange Server 2007 SP2 or later, run the following command from the Exchange Management Shell on the Microsoft Exchange Server machine:

  ```
  Set-TransportConfig -HeaderPromotionModeSetting MayCreate
  ```

  If required, you can return to the previous value of the HeaderPromotionModeSetting property after running the utility.

To specify custom headers:

1. On the main server machine, browse to the folder where the OpenScape Contact Center software is installed, and then double-click **osccmseheaders.exe**. A command prompt window opens.
2. Press **ENTER** to continue.

3. At the **From address** prompt, type the e-mail address that you want to use as the From address to send the special e-mail message, and then press **ENTER**. This must be the e-mail address associated with the user account that is used to authenticate with Microsoft Exchange Server, such as the default OSCCEmail account.
4. At the **To address** prompt, type the e-mail address to which you want to send the special e-mail message, and then press **ENTER**. This should be a known e-mail address on the Microsoft Exchange Server.
5. At the **Subject** prompt, type a subject for the special e-mail message, and then press **ENTER**.
6. At the **SMTP server host name** prompt, type the host name of the Microsoft Exchange Server machine, and then press **ENTER**.
7. At the **SMTP server port number** prompt, type the port number that has been configured for SMTP on the Microsoft Exchange Server machine, and then press **ENTER**.
8. At the **SMTP user name** prompt, type the user name for the Microsoft Exchange Server account that will be used to send the special e-mail message, and then press **ENTER**. The account must be able to send an e-mail message using the From address specified in step 3.
9. At the **SMTP password** prompt, type the password for the Microsoft Exchange Server account that will be used to send the special e-mail message, and then press **ENTER**.

3.5 Planning the IBM Lotus Domino deployment

For the OpenScape Contact Center system to use Lotus Domino, you must configure one IMAP-capable mailbox where user e-mail messages will be delivered. Ensure that you configure the **Format preference for incoming mail** on the mailbox as **Prefers MIME**. For information on how to perform this and other tasks described in this section, refer to the Lotus Domino documentation.

IMPORTANT: The Lotus Domino configuration should only be completed by a trained Lotus Domino Administrator.

If you want to present multiple contact e-mail addresses to your customers, you need to configure an alias for each additional e-mail address that points to the IMAP-capable mailbox. Creating an alias

ensures that e-mail messages sent to the corporate e-mail server are routed to the OpenScape Contact Center E-mail Server mailbox for user handling. For more information, see the *Manager Help*.

Refer to the Lotus Domino Administrator Help for information on:

- Security for configured aliases
- Configuring SMTP routing

IMPORTANT: Ensure that you enable **immediate full text indexing** on the database that you create. If you do not enable immediate full text indexing, IMAP searches will fail, and the performance of the OpenScape Contact Center E-mail Server will be severely affected.

3.5.1 Compacting the database

When you compact the Lotus Domino database, the OpenScape Contact Center E-mail Server identifies the corporate e-mail server as down because IMAP access to the database is interrupted. The type of database compacting that you implement affects how long the OpenScape Contact Center E-mail Server can access the Lotus Domino database. We recommend that you select the **In-place compacting with space recovery only** (-b flag) option. This is the fastest method and only minimally impacts your system.

IMPORTANT: We strongly recommend that you compact the corporate e-mail server database at the OpenScape Contact Center data maintenance time. Performing this maintenance at any other time may adversely affect the processing of e-mail messages within the OpenScape Contact Center system.

3.6 Setting up a secure connection for an e-mail server

To set up a secure (SSL) connection between the corporate e-mail server and the OpenScape Contact Center E-mail Server, you must perform the following tasks:

- Install an SSL certificate and enable SSL security for the incoming (IMAP4) and/or outgoing (SMTP) e-mail messages on the corporate e-mail server machine. Follow the instructions provided by the manufacturer, or contact your e-mail provider for assistance.

  NOTE: Lotus Domino servers allow SSL-secured connections on a given port even if the port is not configured to require the use of SSL. This does not cause any operational issues. However, administrators should be aware that, although OpenScape Contact Center is able to establish a secure connection to the Domino server, this is not a reliable indication that the use of SSL will be enforced for connections established by other e-mail clients. If you require a secure Domino environment, you must check this carefully in the Domino configuration.

- Enable SSL security for the corresponding IMAP server and/or SMTP server in the Manager application. For details, see the *Manager Help*.

We recommend that you obtain the certificate from a recognized certification authority, such as VeriSign, although self-signed certificates are also supported. In either case, the certificate must be a trusted certificate.

NOTE: When you use a certificate which is self generated or generated by a Certificate Authority which is not covered by the default Java keytore and you want to install a new SSL certificate on the corporate e-mail servers, it may be necessary to add the corresponding root+intermediate certificate in the keystore of the JAVA package which is being used by Agent Portal.
The certificate can be added to the keystore by means of the following line command (from the <Java>\bin directory):

```
keytool –import –alias <server_fqdn> -keystore
..\lib\security\cacerts –file <certificate file>
```

3.7 Using authentication on an e-mail server

In the OpenScape Contact Center system, authentication is mandatory for the IMAP server and optional for the SMTP server. The authentication settings specified on the corporate e-mail server must match those specified in the OpenScape Contact Center system.

To enable authentication in Microsoft Exchange:

- Select **Basic Authentication**.
- If you have SSL enabled, be sure to select the option to require encryption.

To enable authentication in IBM Lotus Domino:

- The OpenScape Contact Center system does not use client certificates, so for the SSL Authentication options, ensure that **Client certificate** is set to **No**, and **Name & password** is set to **Yes**.

3.8 Supporting the e-mail reports feature

To use the e-mail reports feature, the OpenScape Contact Center E-mail Server must be able to send e-mail messages, by way of the corporate e-mail server, using a From address that is different than the From address that the OpenScape Contact Center E-mail Server uses to log on to the corporate e-mail server.

The intention is to allow the OpenScape Contact Center E-mail Server to send e-mail messages on behalf of other SMTP e-mail accounts. For example, when the OpenScape Contact Center E-mail Server is logged on to the corporate e-mail server as "oscc@company.com" and an e-mail message is sent on behalf of "manager@company.com", the expectation is that the recipient of the message will see “From: manager@company.com”, and not “From: oscc@company.com on behalf of manager@company.com".

When the corporate e-mail server is configured for SMTP authentication and SMTP relaying is restricted, this functionality can be achieved as follows:

- **Microsoft Exchange Server 2007, 2010, and 2013** – If you need to send e-mail messages from e-mail addresses that are in the same domain, you can give the OpenScape Contact Center E-mail Server account on the corporate e-mail server full permission to each of the OpenScape Contact Center user's mailboxes via Active Directory. You must also create a new contact in the Active Directory with the SMTP e-mail address OSCCEmail@company.com, and then give the OpenScape Contact Center server machine's e-mail account Send As permission for the new contact. For details, see the Microsoft Exchange Server documentation.
- **Microsoft Exchange Server 2007, 2010, and 2013 only** – If you need to send e-mail messages from e-mail addresses that are outside the domain, you can configure a custom Receive connector. For details on how to configure a Receive connector, see the Microsoft Exchange Server documentation.
- **Lotus Domino 8.0 and 8.5** – The only requirement is that you must ensure that the value of the SMTPVerifyAuthenticatedSender setting is 0. For details on this setting, see the Lotus Domino documentation.

4 Configuring the corporate Web server

This chapter describes how to configure the Web component files on the corporate Web server machine to support the OpenScape Contact Center Web collaboration, Web callback, and VoiceXML integration features. It also describes how to set up a secure connection for the corporate Web server machine, localize and customize the default files, and troubleshoot common issues.

IMPORTANT: Before upgrading the files on the corporate Web server machine, copy any customized Web component files to a safe location so that you can reapply them after the upgrade. Failure to do so will result in the loss of any customized files as they are not retained as part of the upgrade process.

NOTE: When creating or customizing Web pages for use with the OpenScape Contact Center Web features, ensure that you take precautions to minimize potential security vulnerabilities.

4.1 System requirements for using Web components

For the Web component files to work properly, you must ensure that the corporate Web server and the Web browser used to access the features, meet the requirements provided in this section.

4.1.1 Corporate Web server requirements

The corporate Web server can use any of the following Web servers and corresponding operating systems:

- Microsoft Internet Information Server (IIS) 8 and 8.5
- Apache Tomcat 6.0 on Red Hat Enterprise Linux 6 Server
- Apache Tomcat 7.0.63 on Red Hat Enterprise Linux 6 Server

4.1.2 Web browser requirements

The following Web browsers have been tested in conjunction with the OpenScape Contact Center system:

- Internet Explorer 6, 7, 8, and 9
- Firefox 10 and 11

For more information on these servers, refer to the manufacturer's documentation.

Ensure that the Web browser is configured as follows:

- Security setting for the Internet is set to medium or lower
- Javascript is enabled
- Popups are enabled (the popup blocker is turned off, or configured to always allow popups from the Web site)

4.2 Configuring Web components

This section describes how to configure the Web components, depending on the type of Web server installed.

NOTE: As a result of the Web Interaction Server configuration, you might have to perform additional configuration of the Web components. For example, you might need to set up a secure connection for a Web server, or customize the Web components. For details, see Section 4.3, "Setting up a secure connection for a Web server", on page 34 and Section 4.4, "Localizing and customizing Web components", on page 37..

4.2.1 Configuring an IIS server

This section describes how to configure the Web components on an IIS server. If you require information about installing and configuring the IIS server itself, refer to the Windows documentation.

NOTE: OpenScape Contact Center uses a heartbeat mechanism to monitor the connection between the corporate Web server and the Web Interaction Server. There are several configurations on an IIS server, such as application pool recycling, that can cause the OpenScape Contact Center ISAPI component to be unloaded. If this happens, the System Monitor application will indicate that the connection is down. To avoid this issue, change the configuration as described in the Windows documentation.

NOTE: When the IIS server is running on a 64-bit operating system, the IIS server must be configured to run 32-bit Web applications because the OpenScape Contact Center ISAPI DLL is 32-bit.

4.2.1.1 Configuring the Web component files on an IIS server

You must copy the Web component files from the OpenScape Contact Center DVD to the corporate Web server machine and then update the files.

To configure the Web component files on an IIS server:

1. Create a folder on the corporate Web server machine to store the Web component files. For example:

   `c:\HPPC`

2. Insert the OpenScape Contact Center DVD into the DVD-ROM drive.
3. On the DVD, browse to the **OpenScape Contact Center Web Components\IIS** folder.
4. Copy the **HPPCEnterpriseWeb.zip** file to the corporate Web server machine and unzip the file to the location you created in step 1. The following file structure is created:

   c:\HPPC\Default.htm

   c:\HPPC\hppcwis.dll

   c:\HPPC\HPWC.ini

   c:\HPPC\html

   c:\HPPC\html\WCCallbackMain.htm

   c:\HPPC\html\WCMain.htm

   c:\HPPC\html\english (and corresponding files)

   c:\HPPC\images (and corresponding files)

   c:\HPPC\VXML (and corresponding files)

   IMPORTANT: Do not change this file structure, as it is required for the files to execute properly.

5. Open the **HPWC.ini** file in a text editor and, under **[HPPCSETTINGS]**, change the **Address** setting to the host name or IP address of the OpenScape Contact Center main server machine.

   NOTE: When the system is configured for high availability (warm standby), you must change the **Address** setting to the cluster name or virtual IP address of the server cluster.

   IMPORTANT: Ensure that the **Port** setting is the same as the port number configured in the Manager application, and that the port is opened in the firewall between the corporate Web server machine and the OpenScape Contact Center main server machine. The default port number is 6021. If you change the port number, you must restart the corporate Web server machine and the Web Interaction Server.

6. Save and close the file.
7. In IIS, create a new virtual directory for the default Web site. For details, see the Windows documentation. When creating the virtual directory, ensure that you:
   - Provide an alias such as HPPC.
   - Select the folder you created in step 1 when the system asks you to specify the Web site content directory.
   - Enable the following access permissions:
     - Read
     - Run scripts (such as ASP)
     - Execute (such as ISAPI applications or CGI)

   IMPORTANT: Ensure that ISAPI extensions have status **allowed** in the Web Service Extensions node in IIS Manager for IIS. Otherwise, when the system attempts to call OpenScape Contact Center ISAPI functionality, error 404 will be returned. To enable or disable the ISAPI extensions individually, see the Microsoft Management Console Help for information relating to enabling and disabling dynamic content in server configurations.

4.2.1.2 Testing Web collaboration on an IIS server

This section describes how to test the Web collaboration functionality on an IIS server.

To test Web collaboration on an IIS server:

1. Open a Web browser and type the URL to access the WCMain.htm demo page. The format of the URL is:

   `http://<hostname>/<VirtualPath>/html/WCMain.htm`

   where

   - `<hostname>` is the host name or IP address of the corporate Web server machine.
   - `<VirtualPath>` is the path to the virtual directory you created.

   For example:

   `http://127.0.0.1/HPPC/html/WCMain.htm`

2. On the WCMain.htm page, click the **Request Web Session** button. If you see a page with the message "You have requested a live Web Collaboration session", you have loaded **CaptureWCData.htm** and successfully configured Web collaboration on the Web server in a basic default configuration.

   NOTE: At this point, if you click the **Submit** button on **CaptureWCData.htm** you may receive an error. You can click this button after the Web server configuration is complete.

   ---

3. Configure the Web Interaction Server on the OpenScape Contact Center main server machine. For details, see the *Manager Help*.

4.2.1.3 Testing Web callback on an IIS server

This section describes how to test the Web callback functionality on an IIS server.

To test Web callback on an IIS server:

1. Open a Web browser and type the URL to access the WCCallbackMain.htm demo page. The format of the URL is:

   `http://<hostname>/<VirtualPath>/html/WCCallbackMain.htm`

   where

   - `<hostname>` is the host name or IP address of the corporate Web server machine.
   - `<VirtualPath>` is the path to the virtual directory you created.

   For example:

   `http://127.0.0.1/HPPC/html/WCCallbackMain.htm`

2. On the WCCallbackMain.htm page, click the **Try Web Callback** button. If a page opens showing fields about customer contact information, then you have loaded **WebCallback.htm** and successfully configured Web callback on the Web server in a basic default configuration.

   NOTE: At this point, if you click the **Submit** button on **WebCallback.htm** you may receive an error. You can click this button after the Web server configuration is complete.

   ---

3. Configure the Web Interaction Server on the OpenScape Contact Center main server machine. For details, see the *Manager Help*.

4.2.1.4 Testing VoiceXML integration on an IIS server

This section describes how to test the VoiceXML integration on an IIS server.

To test VoiceXML integration on an IIS server:

1. Ensure that VoiceXML is defined as a MIME type in the virtual directory properties or in the overall system. For example, to define the MIME type in the virtual directory:

   a) Right-click the virtual directory, and select **Properties**.

   b) Click the **HTTP Headers** tab, and then click **MIME Types**.

c) Click **New**.

d) In the **Extension** box, type `VXML`.

e) In the **MIME type** box, type `application/voicexml+xml`.

f) Click **OK**.

2. Open a Web browser and type the URL to access the Initialize.vxml demo page. The format of the URL is:

   `http://<hostname>/<VirtualPath>/VXML/Initialize.vxml`

   where:

   - `<hostname>` is the host name or IP address of the corporate Web server machine.
   - `<VirtualPath>` is the path to the virtual directory you created.

   For example:

   `http://127.0.0.1:8080/HPPC/VXML/Initialize.vxml`

3. In the dialog box that appears, click **OK** to open the Initialize.vxml file. If you see the Initialize.vxml file, you have successfully configured VoiceXML on the Web server in a basic default configuration.
4. Configure the Web Interaction Server on the OpenScape Contact Center main server machine. For details, see the *Manager Help*.

4.2.2 Configuring a Tomcat server

This section describes how to configure the Web component settings on the Tomcat server. If you require information about installing and configuring the Tomcat server itself, or connecting Tomcat to the Apache server, refer to the Tomcat server documentation.

4.2.2.1 Configuring the .war file on a Tomcat server

This section describes how to configure and deploy the .war file on a Tomcat server.

To configure the .war file on a Tomcat server:

1. Insert the OpenScape Contact Center DVD into the DVD-ROM drive.
2. On the DVD, browse to the **OpenScape Contact Center Web Components\Apache Tomcat** folder.

3. Copy the **HPPCEnterpriseWeb.war** file to the corporate Web server machine.
4. Rename the .war file to a name that is suitable for your environment. In the following instructions, the name of the .war file has been changed to **HPPC.war**. This will deploy the sample Web application called HPPC. The name of the .war file must be capitalized as shown for the sample configuration to work.
5. Ensure that the Java Development Kit (JDK) is installed.
6. To extract the config.properties file to a new folder called hpwcapp, open a command prompt window, change to the directory that contains the HPPC.war file, type the following at the command prompt, and then press **ENTER**:

   ```
   jar xfv HPPC.war hpwcapp/config.properties
   ```

7. Open the **hpwcapp/config.properties** file in a text editor, and do the following:

   - Change the **servlet.name** setting to reflect the name of .war file you specified in step 4. In the sample configuration, the setting is `servlet.name=/HPPC/hppcwebchat`.
   - Change the **socket.server.name** setting to the host name or IP address of the OpenScape Contact Center main server machine.

   NOTE: When the system is configured for high availability (warm standby), you must change the **socket.server.name** setting to the cluster name or virtual IP address of the server cluster.

   NOTE: Ensure that the **socket.server.port** setting is the same as the port number configured in the Manager application, and that the port is opened in the firewall between the corporate Web server machine and the OpenScape Contact Center main server machine. The default port number is 6021. If you change the port number, you must restart the corporate Web server machine and the Web Interaction Server.

   ---

8. Save and close the file.
9. To update the HPPC.war file, at the command prompt in the same directory as in step 6, type:

   ```
   jar ufv HPPC.war hpwcapp/config.properties
   ```

10. Deploy the HPPC.war file on the Tomcat server. For details, see the Tomcat Web Application Manager documentation.

4.2.2.2 Testing Web collaboration on a Tomcat server

This section describes how to test the Web collaboration feature on a Tomcat server.

To test Web collaboration on a Tomcat server:

1. Open a Web browser and type the URL to access the WCMain.htm demo page. The format of the URL is:

   `http://<hostname>/HPPC/html/WCMain.htm`

   where `<hostname>` is the host name or IP address of the corporate Web server machine.

   For example:

   `http://127.0.0.1:8080/HPPC/html/WCMain.htm`

2. On the WCMain.htm page, click the **Request Web Session** button. If you see a page with the message "You have requested a live Web Collaboration session", you have loaded **CaptureWCData.htm** and successfully configured Web collaboration on the Web server in a basic default configuration.

   NOTE: At this point, if you click the **Submit** button on **CaptureWCData.htm** you may receive an error. You can click this button after the Web server configuration is complete.

   ---

3. Configure the Web Interaction Server on the OpenScape Contact Center main server machine. For details, see the *Manager Help*.

4.2.2.3 Testing Web callback on a Tomcat server

This section describes how to test the Web callback feature on a Tomcat server.

To test Web callback on a Tomcat server:

1. Open a Web browser and type the URL to access the WCCallbackMain.htm demo page. The format of the URL is:

   `http://<hostname>/HPPC/html/WCCallbackMain.htm`

   where `<hostname>` is the host name or IP address of the corporate Web server machine.

   For example:

   `http://127.0.0.1:8080/HPPC/html/WCCallbackMain.htm`

2. On the WCCallbackMain.htm page, click the **Try Web Callback** button. If a page opens showing fields about customer contact information, then you have loaded **WebCallback.htm** and successfully configured Web callback on the Tomcat server in a basic default configuration.

   NOTE: At this point, if you click the **Submit** button on **WebCallback.htm** you may receive an error. You can click this button after the Web server configuration is complete.

   ---

3. Configure the Web Interaction Server on the OpenScape Contact Center main server machine. For details, see the *Manager Help*.

4.2.2.4 Testing VoiceXML integration on a Tomcat server

This section describes how to test the VoiceXML integration on a Tomcat server.

To test VoiceXML integration on a Tomcat server:

1. Open a Web browser and type the URL to access the Initialize.vxml demo page. The format of the URL is:

   `http://<hostname>/HPPC/VXML/Initialize.vxml`

   where `<hostname>` is the host name or IP address of the corporate Web server machine.

   For example:

   `http://127.0.0.1:8080/HPPC/VXML/Initialize.vxml`

2. In the dialog box that appears, click **OK** to open the Initialize.vxml file. If you see the Initialize.vxml file, you have successfully configured VoiceXML on the Tomcat server in a basic default configuration.
3. Configure the Web Interaction Server on the OpenScape Contact Center main server machine. For details, see the *Manager Help*.

4.2.3 Configuring a Sun Java System Web Server

This section describes how to configure the Web components on a Sun Java System Web Server. If you require information about installing and configuring the Sun Java System Web Server itself, refer to the Sun documentation.

4.2.3.1 Configuring the .war file on a Sun Java System Web Server

This section describes how to configure and deploy the .war file on a Sun Java System Web Server.

To configure the .war file on a Sun Java System Web Server:

1. Insert the OpenScape Contact Center DVD into the DVD-ROM drive.
2. On the DVD, browse to the **OpenScape Contact Center Web Components\Sun Java System Web Serve**r folder.
3. Copy the **HPPCEnterpriseWeb.war** file to the corporate Web server machine.
4. Rename the .war file to a name that is suitable for your environment. In the following instructions, the name of the .war file has been changed to **HPPC.war**. This will deploy the sample Web application called HPPC. The name of the .war file must be capitalized as shown for the sample configuration to work.
5. To extract the config.properties file to a new folder called hpwcapp, open a command prompt window, change to the directory that contains the HPPC.war file, type the following on the command line, and then press **ENTER**:

   ```
   jar xfv HPPC.war hpwcapp/config.properties
   ```

6. Open the **hpwcapp/config.properties** file in a text editor, and do the following:

   - Change the **servlet.name** setting to reflect the name of .war file you specified in step 4. In the sample configuration, the setting is `servlet.name=/HPPC/hppcwebchat`.
   - Change the **socket.server.name** setting to the host name or IP address of the OpenScape Contact Center main server machine.

   NOTE: When the system is configured for high availability (warm standby), you must change the **socket.server.name** setting to the cluster name or virtual IP address of the server cluster.

   NOTE: Ensure that the **socket.server.port** setting is the same as the port number configured in the Manager application, and that the port is opened in the firewall between the corporate Web server machine and the OpenScape Contact Center main server machine. The default port number is 6021. If you change the port number, you must restart the corporate Web server machine and the Web Interaction Server.

   ---

7. Save and close the file.
8. To update the HPPC.war file, at the command prompt in the same directory as in step 5, type:

   ```
   jar ufv HPPC.war hpwcapp/config.properties
   ```

9. Go to the Sun Java System Web Server administrator site and create a new server instance. To access the administrator site, open a Web browser and type the URL. The format of the URL is:

   ```
   http://<hostname>/https-admserv/bin/index
   ```

   where `<hostname>` is the host name or IP address of the corporate Web server machine.

When creating the server instance, use **HPPC** for the server identifier. This automatically creates a folder called **/https-HPPC**. For details, see the Sun documentation.

NOTE: If you select the **Never attempt to resolve IP addresses into host names** check box, you must be consistent with your configuration. This means using either IP addresses or host names, but not both.

10. Start the new server instance.
11. Deploy the HPPC.war file on the Sun Java System Web Server. For details, see the Sun documentation. When deploying the .war file, the application URL is **/HPPC**.

4.2.3.2 Testing Web collaboration on a Sun Java System Web Server

This section describes how to test Web collaboration on a Sun Java System Web Server.

To test Web collaboration on a Sun Java System Web Server:

1. Open a Web browser and type the URL to access the WCMain.htm demo page. The format of the URL is:

   `http://<hostname>/HPPC/html/WCMain.htm`

   where `<hostname>` is the host name or IP address of the corporate Web server machine.

   For example:

   `http://127.0.0.1:8181/HPPC/html/WCMain.htm`

2. On the WCMain.htm page, click the **Request Web Session** button. If you see a page with the message "You have requested a live Web Collaboration session", you have loaded **CaptureWCData.htm** and successfully configured Web collaboration on the Web server in a basic default configuration.

   NOTE: At this point, if you click the **Submit** button on **CaptureWCData.htm** you may receive an error. You can click this button after the Web server configuration is complete.

3. Configure the Web Interaction Server on the OpenScape Contact Center main server machine. For details, see the *Manager Help*.

4.2.3.3 Testing Web callback on a Sun Java System Web Server

This section describes how to test Web callback on a Sun Java System Web Server.

To test Web callback on a Sun Java System Web Server:

1. Start the server instance you created in Section 4.2.3.1, "Configuring the .war file on a Sun Java System Web Server", on page 31.
2. Open a Web browser and type the URL to access the WCCallbackMain.htm demo page. The format of the URL is:

   `http://<hostname>/HPPC/html/WCCallbackMain.htm`

   where `<hostname>` is the host name or IP address of the corporate Web server machine.

   For example:

   `http://127.0.0.1:8081/HPPC/html/WCCallbackMain.htm`
3. On the WCCallbackMain.htm page, click the **Try Web Callback** button. If a page opens showing fields about customer contact information, then you have loaded **WebCallback.htm** and successfully configured Web callback on the Sun Java System Web Server in a basic default configuration.

   NOTE: At this point, if you click the **Submit** button on **WebCallback.htm** you may receive an error. You can click this button after the Web server configuration is complete.
4. Configure the Web Interaction Server on the OpenScape Contact Center main server machine. For details, see the *Manager Help*.

4.3 Setting up a secure connection for a Web server

The system can be configured to use TLS certificate-based authentication to secure the connection between the Web Interaction Server and the corporate Web server.

This section describes how to enable TLS security on the corporate Web server, according to the type of corporate Web server you have.

To complete the TLS configuration, you must also do the following:

1. Install an TLS certificate on the main server machine. For details, see the *Installation Guide*.
2. In the Manager application, select an TLS-enabled port for the Web connection. For details, see the *Manager Help*.

NOTE: We recommend that you do not enable TLS security on the corporate Web server until all other Web Interaction Server configurations are complete.

4.3.1 Enabling TLS on an IIS server

This section describes how to enable TLS security on an IIS server.

To enable TLS on an IIS server:

1. Open the **HPWC.ini** file in a text editor.
2. Under **[HPPCSETTINGS]**, ensure that the **Address** is set to the host name of the OpenScape Contact Center main server machine, which matches the common name of the TLS certificate.

   NOTE: When the system is configured for high availability (warm standby), you must set the **Address** setting to the server cluster name.

   ---

3. Set the **TLSPort** setting to the port number that will be used by the secure Web features, for example:

   ```
   SSLPort=8443
   ```

   NOTE: Ensure that the port number you configure here matches the TLS port number configured in the Manager application. For details, see the *Manager Help*.

   ---

4. Set the required SSL flags to true:
   - For Web collaboration, `ChatUsesSSL=true`
   - For Web callback, `CallbackUsesSSL=true`

- For VoiceXML, `VoiceXMLUsesSSL=true`

NOTE: When the TLS flag is set to true, the feature will only be available via TLS on the port specified by the TLSPort setting.

---

5. On the **File** menu, click **Save**, and then click **Exit**.

4.3.2 Enabling TLS on a Tomcat or Sun Java server

This section describes how to enable TLS security on a Tomcat Web server or a Sun Java System Web Server.

If required, download Java Secure Socket Extension (JSSE) before you begin. For detailed instructions, see the manufacturer's documentation.

To enable TLS on a Tomcat or Sun Java server:

1. Install the keystore according to the manufacturer's instructions.
2. Open the **config.properties** file in a text editor.
3. Set the **socket.server.name** setting to the host name of the OpenScape Contact Center main server machine, which matches the common name of the TLS certificate.

NOTE: When the system is configured for high availability (warm standby), you must set the **socket.server.name** setting to the server cluster name.

---

4. Set the **socket.server.port.ssl** setting to the port number that will be used by the secure Web features, for example:

   ```
   socket.server.port.ssl=8443
   ```

NOTE: Ensure that the port number you configure here matches the TLS port number configured in the Manager application. For details, see the *Manager Help*.

---

5. Set the required SSL flags to true:
   - For Web collaboration, `socket.webchat.ssl=true`
   - For Web callback, `socket.webcallback.ssl=true`
   - For VoiceXML (Tomcat only), `socket.voicexml.ssl=true`

   NOTE: When the TLS flag is set to true, the feature will only be available via SSL on the port specified by the **socket.server.port.ssl** setting.

6. On the **File** menu, click **Save**, and then click **Exit**.

4.4 Localizing and customizing Web components

After you have tested the corporate Web server, you can localize and then customize the Web component files for your environment.

4.4.1 Localizing Web components

After you have tested the corporate Web server, you can localize the Web component files to the language that is supported on your Web site. The example below shows a localization procedure for the German language.

To localize the Web component files:

1. Create a new subdirectory under the html directory of the existing directory structure that is shown in step 4 of Section 4.2.1.1, “Configuring the Web component files on an IIS server”. For example:

   `c:\HPPC\html\deutsch`

2. Copy all of the default files in `c:\HPPC\html\english` to your new directory.
3. In your new directory, use an appropriate tool to update the text or graphics of the pages as appropriate, and save your files with the same name. For example, you may want to update the text and buttons in CallMePage.htm for your own localization requirements.

   IMPORTANT: If you use non-ASCII symbols in the updated pages, they should be saved in a UTF-8 format.

4. Create a copy of WCMain.htm within the same directory and rename it. For example, you can rename WCMain.htm to WCDeutsch.htm:

   `c:\HPPC\html\WCDeutsch.htm`

5. Update the URL used by the page (in the example, WCDeutsch.htm) to point to the new directory. To do so, you will change "english" to the correct language. For example:

   `?varUserRequest=REQ_WEBCHAT_MAIN&varUserLanguage=`**`deutsch`**

6. Test the new page (for example, WCDeutsch.htm by clicking the **Need Live Help?** button. If you see **CaptureWCData.htm**, then you have successfully localized the WCMain.htm page.

4.4.2 Customizing Web components

After you have localized WCMain.htm, you must customize the CaptureWCData.htm file as it contains the elements required for OpenScape Contact Center to connect a Web collaboration customer with the appropriate user. This file also contains visual presentation elements of the Web collaboration session, such as greetings and icons, that can be customized.

You must have one CaptureWCData.htm file for each language that you localized, and each CaptureWCData.htm file must be located in the appropriate language directory. For example:

c:\HPPC\html\english\CaptureWCData.htm

c:\HPPC\html\deutsch\CaptureWCData.htm

The actual CaptureWCData.htm page that is activated depends on the language indicated in the WCMain.htm page. For example:

?varUserRequest=REQ_WEBCHAT_MAIN&varUserLanguage=english

?varUserRequest=REQ_WEBCHAT_MAIN&varUserLanguage=deutsch

The following table shows the parameters in CaptureWCData.htm that can be updated.

IMPORTANT: You cannot delete any of the parameters in the captureWCData.htm file. The VarUserRequest parameter and the standard buttons cannot be modified or removed.

Name/ID	Description	Detail
varUserLanguage	Defines pages used during the Web collaboration session.	This is the subdirectory of the html directory (see Section 4.4.1, "Localizing Web components").
varHPPCLanguage	The name of the Web collaboration language. Used to define the set of rules (standard messages, emoticons, and so on) for Web collaboration sessions.	The value must correspond to a Web collaboration language defined in the Manager application.
varSessionPriority	The priority of the contact. Used by the Web collaboration workflow during routing.	The value must be between 1 and 100.
varCustomerName	Customer name.	No limitation.
varSource	The source of the contact. Used by the Web collaboration workflow during routing.	The value must be in one of the languages supported by the OpenScape Contact Center system. Non-ASCII characters, non-printable ASCII characters, and the following special characters are not allowed: accent grave (`), asterisk (*), comma (,), double quotation mark ("), exclamation mark (!), percentage sign (%), pipe (|), and underscore (_).
varDestination	The destination of the contact. Used by the Web collaboration workflow during routing.	The value must be in one of the languages supported by the OpenScape Contact Center system.
varCaption	Customer's question.	No limitation.

Table 1 CaptureWCData.htm parameters

Name/ID	Description	Detail
varBusinessUnitName	In a multitenant environment, the name of the business unit to which incoming Web collaboration contacts belong.	The value must correspond to one of the business units defined in the OpenScape Contact Center system. In a non-multitenant environment, this value can be ignored.

Table 1 CaptureWCData.htm parameters

You can also update other elements, such as Key1 and Key2, as well as add new elements in one of the languages supported by OpenScape Contact Center. All additional elements will add keys and values into the contact data collection of the Web collaboration request, and will be used by the Web collaboration workflow.

4.5 Troubleshooting Web collaboration

This section provides solutions to some of the more common issues you may encounter with Web collaboration.

4.5.1 Web server configuration issues

We recommend that you consider the following issues when configuring Web collaboration settings on your corporate Web server:

- Ensure that the port number is the same as the port number defined in the Manager application.
- Ensure that the IP address for the corporate Web server points to the OpenScape Contact Center main server machine.

NOTE: These settings can be configured in the `HPWC.ini` on the IIS server or `config.properties` on the Tomcat or Sun Java System Web Server.

4.5.2 General connection issues

Some general connection issues and solutions are provided.

Issue: You cannot load the start page or you receive a 404 error message.

Solution: Ensure that the host name can be mapped to its IP address correctly. If it can, ensure that the corporate Web server is running, and that the URL you are using is correct.

NOTE: If you are using a Tomcat server and receive this error, proceed to the `[tomcat-root]/bin` directory and then type `./startup.sh` to restart the corporate Web server machine.

Issue: You are receiving a connection error (error code 1003).

Solution: Ensure that the Web Interaction Server is running properly, and that the IP and port number in your configuration file is correct. These settings can be configured in the `HPWC.ini` on the IIS server or `config.properties` on the Tomcat or Sun Java System Web Server.

You should also ensure that the host name of the Web Interaction Server can be resolved properly on the corporate Web server.

A connection error may also occur if you do *not* have an SSL certificate installed on the Web Interaction Server and the secure setting is turned on. If this is the case, you must either install a server certificate or use the Manager application to turn off the secure setting.

NOTE: On a Tomcat or Sun Java System Web server, the installation of the JSSE library is mandatory regardless of whether you use a secure or plain connection. Since there may be more than one Java Runtime Engine (JRE) installed on your corporate Web server, you must ensure that the JSSE library is installed in the same JRE directory that your corporate Web server is using. For example, the Sun Java System Web Server allows you to configure the path to your Java Runtime Engine (JRE) in the **start-jvm** file located in the Sun Java System Web Server's `https-admserv` directory. For more information, see the manufacturer’s documentation.

4.6 Web callback error codes

The following table lists the error codes that you might encounter while using the Web callback feature. If the system returns any of the error codes listed in the table, the callback is not created.

In addition to the error codes listed in the table, you might also encounter various Callback Server errors that are described in the System Monitor application.

Error Code	Description
1000	A general error has occurred.
1002	Failed to connect to the Web Interaction Server.
1003	The connection to the Web Interaction Server has failed.
1006	The Web page cannot be accessed.
1007	An invalid session ID has been detected.
1008	JavaScript is not enabled.
1010	A mandatory parameter is incorrect.
1011	A parameter is incorrect.
1012	There is an internal error with the Web Interaction Server.
1013	Allocation error.
17006	A duplicate callback was found in the database.
17021	The Callback Server cannot process a request due to an internal error.
17025	A general error has occurred.
17027	The callback queue does not exist.
17028	A callback schedule is invalid.
17029	A callback schedule occurs outside the callback routing schedule configured for the contact center.
17030	The customer name is too long. The maximum is 75 characters.
17031	A telephone number is one of the numbers defined as an excluded number.
17032	The callback description is too long. The maximum is 100 characters.
17033	The contact data is too long. The maximum is 1000 characters.
17035	The priority is invalid. The priority must be between 1 and 100.
17040	A callback schedule has expired.
17047	A callback schedule start or end date is invalid. A callback cannot be scheduled more than 180 days in the future.

Table 2 Web Callback Error Codes

5 Configuring the presence integration

This chapter describes the items that must be configured to support the presence integration feature. The presence integration feature enables Client Desktop users to view the presence of various users via the directory feature.

When the presence integration feature is enabled in the Manager application, and the Client Desktop user performs a directory search, the system attempts to obtain the presence of each entry in the search results, as follows:

- The system first attempts to obtain the user presence state and voice media presence state from the OpenScape Unified Communications (UC) Application, only when the OpenScape UC Application Integration feature is enabled and configured.
- If the user is not an OpenScape UC Application user, or the OpenScape UC Application integration feature is not enabled or is not available, the system attempts to obtain the user presence state from the OpenScape Contact Center system.
- If the user is not an OpenScape Contact Center user or the presence state is not available from the OpenScape Contact Center system, and the system is connected to an OpenScape Voice communication platform, the system attempts to obtain the line state of the user's device from the OpenScape Voice communication platform.

If you are working in a networked environment, you can access the presence for users at the local site only.

5.1 Configuring an OpenScape UC Application user account

To enable the system to integrate with the OpenScape UC Application, you must configure a user account in the OpenScape UC Application that the OpenScape Contact Center system can use to access and maintain connectivity with the OpenScape UC Application. This user account is specified when you configure the presence integration options in the Manager application. For details on how to configure a new user account, refer to the OpenScape UC Application documentation.

5.2 Configuring the external LDAP directory

To enable Client Desktop users to view the presence of other users, you must configure the external LDAP directory to support the display of presence.

Specifically, you must configure one or more of the following fields in the directory:

- **Presence ID** (the OpenScape UC Application user ID)
- **User name** (the OpenScape Contact Center user name)
- **Line State** (the OpenScape Voice line state, only applicable if the system is connected to an OpenScape Voice communication platform)

For details on configuring fields, refer to the LDAP directory's documentation.

6 Maintaining the system

This chapter describes how to perform ongoing maintenance of the OpenScape Contact Center system, including shutting down the main server machine, changing the passwords, and backing up the database.

Remote service access to a main server machine or a central reporting server machine is provided by the Smart Services Delivery Platform (SSDP) Service Plug-in. The SSDP Service Plug-in software is installed automatically on the server machine as part of the installation process. To configure the SSDP Service Plug-in, follow the instructions provided in the SSDP Service Plug-in documentation, which is located on the OpenScape Contact Center DVD in the Utilities\OpenScape Service Plug-in folder.

NOTE: When performing general system maintenance procedures, such as upgrading the network, we recommend that you shut down the OpenScape Contact Center main server machine before proceeding. For special instructions, refer to Section 6.1, "Shutting down a server machine for system maintenance".

NOTE: When the system is configured for high availability (warm standby), stopping the service OpenScape Contact Center from the Services window does not result in a failover.

6.1 Shutting down a server machine for system maintenance

When you need to shut down or restart an OpenScape Contact Center server machine that is running Informix for maintenance purposes, Informix sometimes does not have time to stop the Informix IDS service before the Windows operating system shuts down. If this occurs, the database can become corrupted. To prevent this issue, we recommend that you always stop the Informix IDS service before shutting down or restarting the server machine.

NOTE: To ensure that the database does not become corrupted, always stop the Informix IDS service before shutting down or restarting a server machine.

6.2 Changing the OpenScape Contact Center and Informix passwords

If you need to change the OpenScape Contact Center or Informix passwords for any reason, you must update the passwords in the following three locations:

- Services window
- Computer Management window
- OpenScape Contact Center Startup Configuration window (or System Monitor application)

IMPORTANT: The OpenScape Contact Center and Informix passwords should be changed only under the guidance of your support representative.

The Informix password cannot exceed 16 characters and cannot contain any spaces.

To change the OpenScape Contact Center and Informix passwords:

1. Open the **Services** window.
2. To change the OpenScape Contact Center password, do the following:
   a) Stop the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services.
   b) For each service, open the service and provide the new password on the **Log On** tab.
3. To change the Informix password, do the following:
   a) Stop the following services: **IBM Informix Dynamic Server Message Service**, **Informix IDS - ol_*servername*** (where *servername* is the name of the OpenScape Contact Center server machine), and **Informix Server Discovery Process for SNMP**.
   b) Open the **Informix IDS - ol_*servername*** service and provide the new password on the **Log On** tab.
   c) Open the **Informix Server Discovery Process for SNMP** service and provide the new password on the **Log On** tab.
4. Close the **Services** window.
5. Open the **Computer Management** window.

6. Under **System Tools**, expand **Local Users and Groups**, and then click **Users**.
7. To change the OpenScape Contact Center password, right-click **hppc**, click **Set Password**, and provide the new password.
8. To change the Informix password, right-click **informix**, click **Set Password**, and provide the new password.
9. Close the **Computer Management** window.
10. Open a command prompt window.
11. On the command line, type `tcfmain` and then press **ENTER**. The **OpenScape Contact Center Startup Configuration** window is displayed.
12. To change the Informix password, click the **Administration Server** tab and type the new password in the **Database Server Password** box.

NOTE: When the system is running, you can also change the Informix password by configuring the startup data for the Administration Server using the System Monitor application. For detailed information, see the *System Monitor Help*.

---

13. Close the **OpenScape Contact Center Startup Configuration** window.
14. Start the following services: **IBM Informix Dynamic Server Message Service**, **Informix IDS - ol_*servername*** (where *servername* is the name of the OpenScape Contact Center server machine), and **Informix Server Discovery Process for SNMP**.
15. Start the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services.

6.3 Backing up the database

You should back up the OpenScape Contact Center database on a regular basis, and any time you change the system configuration, to ensure that the data is protected in the event of a failure or corruption. Since the database can be quite large, we recommend that you back up the database only during periods of very low contact volume.

NOTE: In addition to backing up the OpenScape Contact Center database, we recommend that you back up all data on the server machine using a backup utility. Ensure that the backup contains the server machine's System State data, which includes items such as the registry and boot files.

NOTE: When the system is configured for high availability (warm standby), ensure that you back up the primary server machine, the backup server machine, and the optional central reporting server machine.

There are two types of backups you can perform:

- **Full backup** – To limit the potential loss of data to no more than one day, we strongly recommend that you perform a full backup on a daily basis. At the very least, you should back up the database once a week.
- **Incremental backup** – To minimize the potential loss of data between full database backups, you can perform an incremental backup. For example, if you run a full backup at night, you can run an incremental backup during the day. The incremental backup takes less time, because it only backs up the changes since the start of the last full backup.

NOTE: Some of the procedures in this section are written based on the assumption that you are familiar with using Informix. For detailed instructions, see the Informix documentation provided at the following location:
http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp

---

6.3.1 Scheduling a database backup

You can use the Task Scheduler in Windows Server 2022, 2019, 2016, 2012/2012 R2, to schedule a task that will back up the OpenScape Contact Center database. This section provides guidelines on how to schedule a task. For detailed instructions, see the Microsoft documentation.

IMPORTANT: Scheduled backups use the batch files FULLBACKUP.BAT and INCREMENTALBACKUP.BAT, both of which use the Informix ontape utility to perform the backup. Therefore, before the first scheduled backup runs, you must edit the ontape parameters as described in step 2 on page 51.

NOTE: When the system is configured for high availability (warm standby), we recommend that you schedule the backups on the primary server machine, the backup server machine, and the optional central reporting server machine at the same time to ensure that the backed up data is consistent.

To schedule a database backup:

1. Using the Task Scheduler in Windows Server 2022, 2019, 2016, 2012/2012 R2, schedule a task according to the following guidelines:
   - Select the action **Start a program**, and then select one of the following batch files, which are located in the folder where you installed the OpenScape Contact Center software:
     - To schedule a full backup, select **FULLBACKUP.BAT**.
     - To schedule an incremental backup, select **INCREMENTALBACKUP.BAT**.
   - Specify the user account and password under which to run the task according to the type of operating system:
     - For Windows Server 2022, 2019, 2016, 2012/2012 R2, specify a local Administrator account.
   - To write the results of the backup to a text file, in the task properties, add the argument **<return.txt >results.txt**. Ensure that the folder where the results.txt file is written (normally the folder where you installed the OpenScape Contact Center software) has Read access for Everyone. In Windows Server 2022, 2019, 2016, 2012 or Windows Server 2012 R2,

when you add the argument, you must also specify the path to start in. Ensure that you do not use quotation marks when you specify the path.

6.3.2 Backing up the database using the ontape utility

You can back up the OpenScape Contact Center database to a local tape drive or a local or network drive using the Informix ontape utility.

6.3.2.1 Backing up the database to a local tape drive

This section describes how to back up the OpenScape Contact Center database to a local tape drive using the Informix ontape utility.

To back up the database to a local tape drive:

1. Log on to the server machine where Informix is installed
2. Insert a blank tape into the tape drive of the server machine.
3. Open an Informix command prompt window using the **ol_*servername*** shortcut, where *servername* is the name of the OpenScape Contact Center server machine.
4. To start the backup, do one of the following:
   - For a full backup of the Informix database, at the command prompt, type `ontape -s -L 0`, and then press **ENTER**.
   - For an incremental backup of the Informix database, at the command prompt, type `ontape -s -L 1`, and then press **ENTER**.

   NOTE: The `-s` parameter directs the ontape utility to create a backup and the `-L` parameter specifies the level of the archive, either `0` for full or `1` for incremental.
5. If there is not enough space on the current tape, the system prompts you to insert another tape. If prompted, remove the tape and label it with the date, time, level, and number of the tape in the sequence. Insert another tape, and then press **ENTER**. Repeat this process for as many tapes as required.

6.3.2.2 Backing up the database to a local or network drive

This section describes how to back up the OpenScape Contact Center database to a local or network drive using the Informix ontape utility.

To back up the database to a local or network drive:

1. Log on to the server machine where Informix is installed
2. Edit the ontape parameters as follows:
   - Open the **ONCONFIG.ol_*servername*** file, where *servername* is the name of the OpenScape Contact Center server machine where Informix is installed, in a text editor, such as Notepad. This file is normally located in the Program Files\Informix\etc folder.
   - In the TAPEDEV parameter, specify the path and file name of the backup file on the local or network drive in 8.3 (short) format, for example, C:\Backups\Backup.001. You must ensure that the backup file exists in the specified location before you start the backup, and that the logged on user has at least Modify permission for the backup file. If the backup file does not exist, you can create an empty file using a text editor such as Notepad.
   - In the TAPESIZE parameter, specify 0 so that the backup file does not have a maximum size.
3. Open an Informix command prompt window using the **ol_*servername*** shortcut, where *servername* is the name of the OpenScape Contact Center server machine.
4. To start the backup, do one of the following:
   - For a full backup of the Informix database, at the command prompt, type `ontape -s -L 0`, and then press **ENTER**.
   - For an incremental backup of the Informix database, at the command prompt, type `ontape -s -L 1`, and then press **ENTER**.

NOTE: The `-s` parameter directs the ontape utility to create a backup and the `-L` parameter specifies the level of the archive, either `0` for full or `1` for incremental.

6.3.3 Restoring the database using the ontape utility

This section describes how to restore previously backed up OpenScape Contact Center data using the Informix ontape utility.

NOTE: If you performed an incremental backup, you need the most recent full backup, as well as the incremental backup.

NOTE: When you want to restore L0 backup with an OSCC clean installation, verify whether all chunk files listed by ontape utility exist in the Contact Center Data folder. When they do not, create those files without extension by right-clicking, navigate to **New -> Text Document**, then rename it and delete the extension. Import will not work properly in case those chunk files are not there.

To restore the database using the ontape utility:

1. Log on to the server machine where Informix is installed
2. Stop the following services:
   - **OpenScape Contact Center**
   - **Informix IDS - ol_*servername,*** where *servername* is the name of the OpenScape Contact Center server machine
3. Do one of the following:
   - If you are restoring the data from a tape, insert the first tape of the Full archive that you want to restore into the tape drive of the server machine.
   - If you are restoring the data from a backup file on a local or network drive, ensure that the path and file name of the backup file is configured correctly in the ONCONFIG.ol_*servername* file.
4. Open an Informix command prompt window using the **ol_*servername*** shortcut, where *servername* is the name of the OpenScape Contact Center server machine.
5. On the command line, type `ontape -r`, and then press **ENTER**.
6. When prompted to load a tape, press **ENTER**.
7. When prompted, **Continue restore (Y/N)?**, press **Y**.
8. When prompted to back up the logs, press **N**.

9. If you created an incremental archive, when prompted with **Restore a level 1 archive**, press **Y**. If you did not create an incremental archive, press **N**.
10. When prompted to restore log tapes, press **N**.
11. When the restoration process completes, if you restored the data from a tape drive, remove the last tape from the tape drive.
12. On the command line, type `onmode -m`, and then press **ENTER**. This command places Informix back into its regular mode and may take several minutes to complete.
13. On the command line, type `onstat -r`, and then press **ENTER**. This displays information about the Informix Server environment. The first line indicates the Informix application mode, and should read **On-Line**. To stop the onstat process, press **CTRL+C**.
14. To close the command prompt window, type `exit`, and then press **ENTER**.
15. Close any other windows or applications.
16. Restart the **OpenScape Contact Center** service.

6.3.4 Restoring a zero level backup made using ontape utility

This section describes how to restore a zero level backed up OpenScape Contact Center data using an automated process.

1. To use the zero level restore script, copy the FullRestore.bat, fullrestore.in and replace.vbs files to the server machine. The files are included in the DVD.
2. Open a command prompt as Informix user
3. Run the FullRestore.bat specifying the arguments /tapedev <path> /tapesize<size>, where <path> is the path to the Informix zero level backup, the specify <size> as zero unless you are using an external tape device.

6.3.5 Backing up the database using the onbar utility

This section describes how to back up the OpenScape Contact Center database to a local drive using the Informix onbar utility. The Informix onbar utility can interface directly with the Informix Storage Manager (ISM) or another third-party storage manager application, such as Veritas, to provide a flexible backup solution.

NOTE: You must configure the storage manager application prior to running the onbar utility. For detailed instructions, see the *IBM Informix Storage Manager Administrator's Guide* or the third-party storage manager documentation. The Informix documentation is provided at the following location:
http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp

---

To back up the database to a local drive:

1. Log on to the server machine where Informix is installed
2. Open an Informix command prompt window using the **ol_*servername*** shortcut, where *servername* is the name of the OpenScape Contact Center server machine.
3. To start the backup, do one of the following:
   - For a full backup of the Informix database, at the command prompt, type `onbar -b -L 0`, and then press **ENTER**.
   - For an incremental backup of the Informix database, at the command prompt, type `onbar -b -L 1`, and then press **ENTER**.

NOTE: The `-b` parameter directs the onbar utility to create a backup and the `-L` parameter specifies the level of the archive, either `0` for full or `1` for incremental.

6.3.6 Restoring the database using the onbar utility

This section describes how to restore previously backed up OpenScape Contact Center data using the Informix onbar utility.

NOTE: If you performed an incremental backup, you need the most recent full backup, as well as the incremental backup.

To restore the database using the onbar utility:

1. Log on to the server machine where Informix is installed
2. Open an Informix command prompt window using the **ol_*servername*** shortcut, where *servername* is the name of the OpenScape Contact Center server machine.
3. On the command line, type `onbar -r`, and then press **ENTER**.

6.4 SNMP support

The system supports two methods of generating information that can be viewed by a SNMP management system:

- **OpenScape Contact Center SNMP extension agent** – Exposes OpenScape Contact Center specific information pertaining to the status of OpenScape Contact Center managed objects. This method is supported on the main server machine only.
- **OpenScape CAP Fault Management software** – Acts as a SNMP extension agent to generate SNMP trap messages on behalf of the OpenScape Contact Center software via Windows event logs. This method is supported on the main server machine and the optional central reporting server machine.

The Windows SNMP service must be installed and running on the server machine to support these methods.

The Windows SNMP service must also be installed and running on the main and central reporting server machines to support subscription licensing.

NOTE: You should configure the Windows SNMP service such that the list of community names does not contain “public” or "private", and the list of hosts only contains the hosts that are required to access the information.

6.4.1 OpenScape Contact Center SNMP extension agent

The OpenScape Contact Center SNMP extension agent (osccsnmp.dll) supports standard SNMP requests for Object IDs (OIDs). The SNMP extension agent exposes OpenScape Contact Center specific information pertaining to the status of OpenScape Contact Center managed objects. The information can then be requested by any SNMP management system.

NOTE: It is the responsibility of the user of the SNMP management system to ensure that information can be requested and retrieved from the OpenScape Contact Center SNMP extension agent.

The OpenScape Contact Center specific information that is exposed by the OpenScape Contact Center SNMP extension agent is defined in the sen-oscc-mib.mib file, which maps the managed objects to their respective OIDs. The information that is exposed includes the Call Director extension usage, the number of logged on users, and the number of current and recent contacts. For details on all the information that is available, see the sen-oscc-mib.mib file, which can be viewed using a text editor.

The OpenScape Contact Center specific information can be used to monitor the status of the system. For example, a technician in the network operations center can create a view which generates an alarm when the number of operational voice processor extensions falls below a configured threshold percentage of the total number of configured voice processor extensions. The technician can then notify the customer so that the customer has time to resolve the issue and avoid running out of extensions.

The osccsnmp.dll and sen-oscc-mib.mib files are located in the default installation folder on the main server machine. The osccsnmp.dll file is also used to support subscription licensing.

NOTE: The osccsnmp.dll file is automatically registered on the server machine during installation of the OpenScape Contact Center server software. If the Windows SNMP service is uninstalled, the osccsnmp.dll file will be unregistered. To re-register the .dll file, use the utility program osccregistersnmpextension.exe, which is located in the default installation folder on the main server machine.

6.4.2 OpenScape CAP Fault Management software

The OpenScape CAP Fault Management software is an optional component that can be used to generate OpenScape Contact Center SNMP trap messages. The OpenScape CAP Fault Management software can be installed automatically during the OpenScape Contact Center installation process, or it can be installed manually from the \OpenScape CAP\Fault Management folder on the OpenScape Contact Center DVD.

NOTE: For details on how to configure the OpenScape CAP Fault Management software, see the OpenScape CAP Fault Management documentation.

There are two OpenScape CAP Fault Management configuration files:

- **capfm_procenter.ini** – This the default configuration file that is installed when you install the OpenScape Contact Center server software. It triggers the generation of SNMP trap messages for all OpenScape Contact Center messages.
- **capfm_procenter_service.ini** – This is the service configuration file that should be used if you want to generate SNMP trap messages for only the subset of messages that are relevant to the Network Operations Center.

Both configuration files are located in the \Utilities\Install folder on the OpenScape Contact Center DVD.

7 Managing a central reporting environment

This chapter describes the actions that can be taken if you encounter issues when the system is configured for central reporting.

7.1 Managing replication for central reporting

If there is an issue with replication, you can use the OpenScape Contact Center replication configuration application (trcdbins.exe) to manage data replication.

NOTE: If the system is configured for high availability (warm standby), follow the procedures described in Section 8.1, "Managing replication for high availability (warm standby)", on page 73.

IMPORTANT: The computer clocks on the central reporting server machine and the OpenScape Contact Center server machines that are participating in central reporting must be synchronized. You must synchronize the computer clocks before running the OpenScape Contact Center replication configuration application (trcdbins.exe), and ensure that the clocks remain synchronized. Replication will fail if the times differ by more than two seconds.

7.1.1 About the replication buffer

There are potentially two types of data replication:

- **Central reporting replication** – Replication of the historical reporting data to the central reporting server machine when the system is configured for central reporting.
- **High availability (warm standby) replication** – Replication of the administration and processing data between the primary and backup server machines when the system is configured for high availability (warm standby).

If either replication is interrupted (for example, there is an issue with the network), the data will be stored in the replication buffer. The replication buffer is sized to accommodate approximately two days of central reporting and high availability (warm standby) replication data for an average system.

Based on the buffer capacity, the system performs the following actions:

- **Buffer 50% full** – Issues an error message every hour indicating the percentage of space used in the replication buffer.
- **Buffer 75% full** – Issues an error message every 15 minutes. When the system is configured for both central reporting and high availability (warm standby), and only one type of replication is causing the buffer to fill up, it also stops that replication.
- **Buffer 95% full** – Issues a warning message every 15 minutes and stops replication configured on the server machine.

IMPORTANT: When the system stops replication automatically, you must follow the appropriate procedures to shut down and restart replication manually after the issue has been resolved. Replication will not restart automatically. For details, see Section 7.1.3, "Shutting down all replication for central reporting", on page 63 or Section 8.1.5, "Shutting down all replication", on page 83.

We recommend that you use the System Monitor application to monitor the capacity of the replication buffer and, when necessary, suspend the replication that is causing the issue. For details, see Section 7.1.2, "Suspending replication for central reporting", on page 60, or Section 8.1.1, "Suspending high availability (warm standby) replication", on page 73.

NOTE: The replication buffer will continue to fill up even when replication has been suspended.

7.1.2 Suspending replication for central reporting

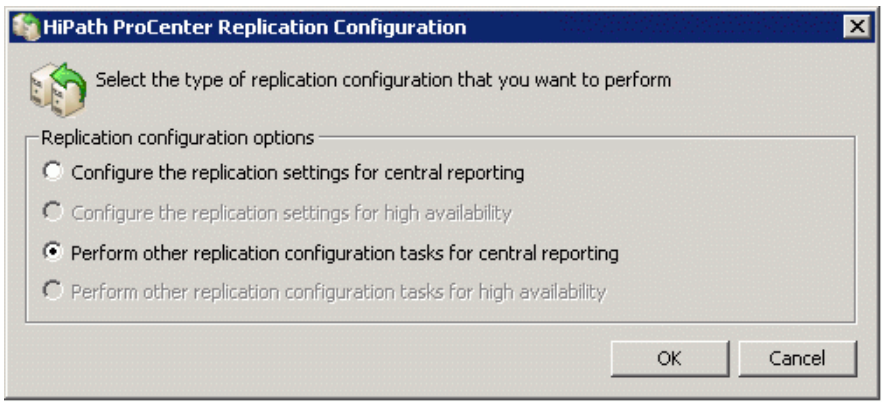
You can suspend the flow of replicated data to the central reporting server machine, for example, to perform maintenance on the network or on the central reporting server machine. We recommend that you suspend replication if you expect the flow of replicated data to be interrupted for more than half a day.

Suspending replication with the central reporting server machine is useful for a couple of reasons:

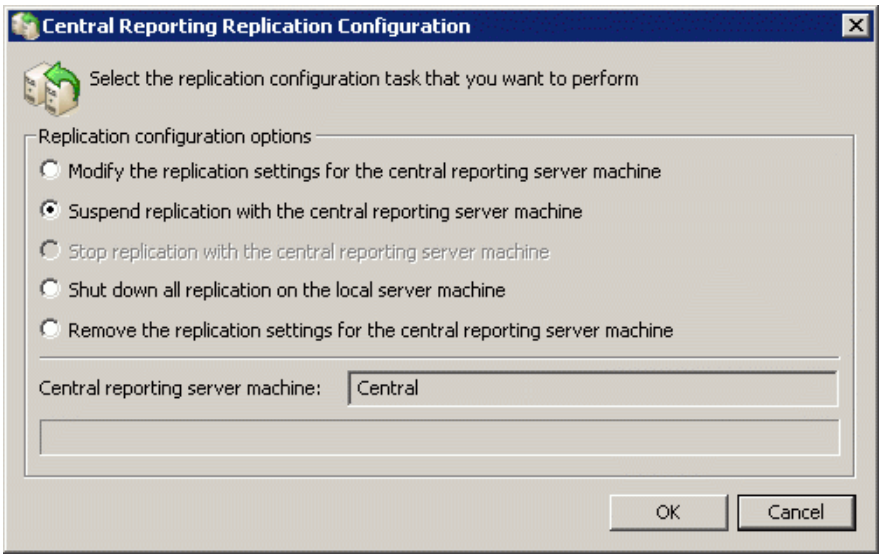
- If a large amount of data accumulates in the buffer during an interruption, significant network and CPU resources will be consumed on the target machine when replication resumes. Suspending replication allows you to resume replication during periods of low contact volume, reducing the impact on the system.
- After an interruption, the data is automatically synchronized. There are two phases of synchronization – the Informix internal data, and the OpenScape Contact Center reporting data. Suspending replication of the reporting data allows the Informix internal data to synchronize first, which allows the system to resume more gracefully.

To suspend central reporting replication:

1. Log on to the server machine where you want to suspend replication.
2. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
3. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.



4. Select **Suspend replication with the central reporting server machine**, and then click **OK**.



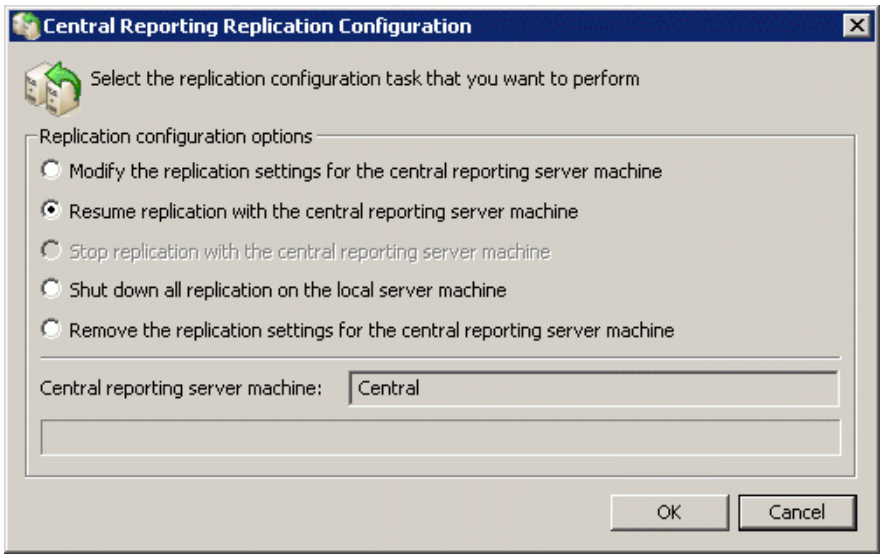
7.1.2.1 Resuming central reporting replication

If the replication buffer contains a large amount of data, we recommend that you resume replication during a period of low contact volume to reduce the impact on the system.

To resume replication with the central reporting server machine:

1. Log on to the server machine where you previously suspended replication.
2. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
3. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.

4. Select **Resume replication with the central reporting server machine**, and then click **OK**.



7.1.3 Shutting down all replication for central reporting

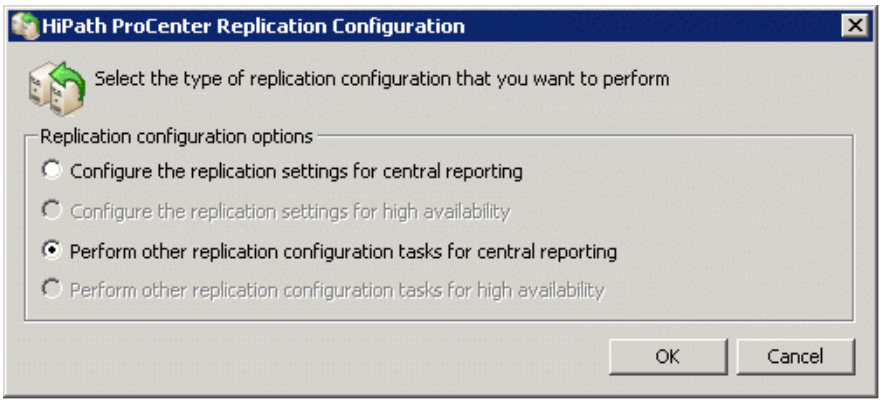
You can shut down replication with the central reporting server machine, for example, if there is an issue with the network and you need to remove the replication settings (which requires network access).

IMPORTANT: You should perform this procedure only when necessary or when instructed to do so because it may require that you synchronize the reporting data. For details, see Section 7.2, "Synchronizing the reporting data for central reporting", on page 66. Whenever possible, we recommend that you suspend rather than shut down replication, because suspending does not require you to synchronize the reporting data.

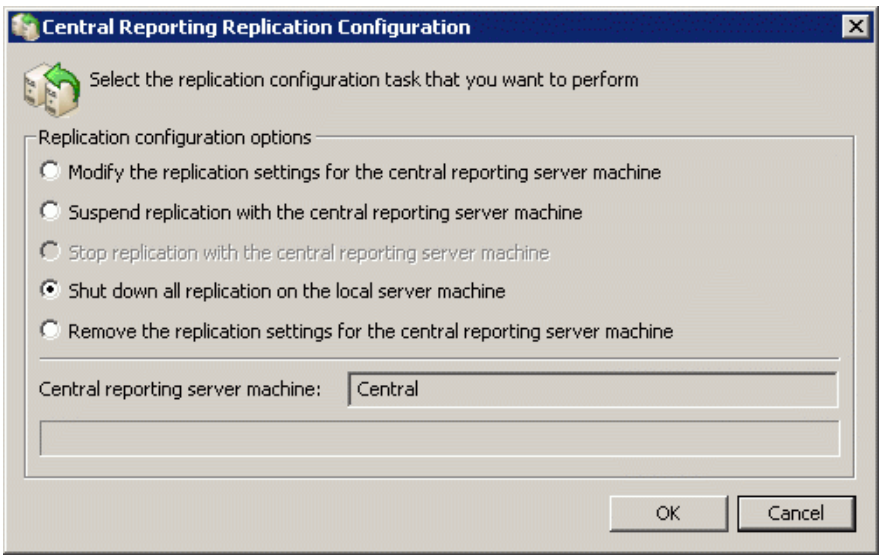
To shut down central reporting replication:

1. Log on to the server machine where you want to shut down replication.
2. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.

3. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.



4. Select **Shut down all replication on the local server machine**, and then click **OK**.

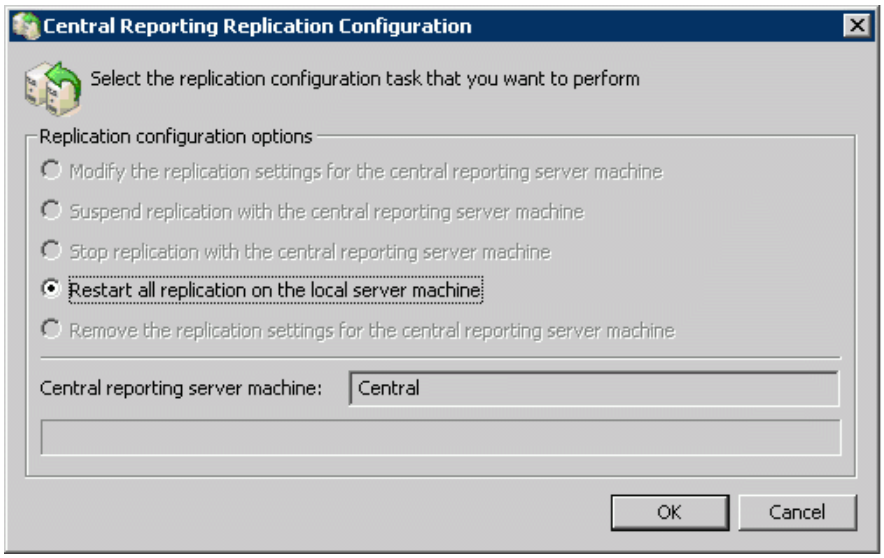


7.1.3.1 Restarting central reporting replication

After replication with the central reporting server machine has been shut down, you can restart it as described in this procedure. During the restart process, all data is removed from the replication buffer.

To restart central reporting replication:

1. Stop the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services on all server machines that are participating in central reporting. Wait for the services to completely shut down before proceeding.
2. Log on to the server machine where you previously shut down replication.
3. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
4. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.
5. Select **Restart all replication on the local server machine**, and then click **OK**.



6. Synchronize the reporting data, only if required. Section 7.2, “Synchronizing the reporting data for central reporting”, on page 66.

7.2 Synchronizing the reporting data for central reporting

If you encounter issues with the historical reporting data, you can synchronize the reporting data. For example, if you are missing data because there has been a lengthy network interruption between one of the OpenScape Contact Center server machines that is participating in central reporting and the central reporting server machine, you can synchronize the reporting data between the server machine and the central reporting server machine.

NOTE: Synchronizing the reporting data can take a very long time. We recommend that you perform this procedure only when the issues with the historical reporting data are unacceptable for your purposes.

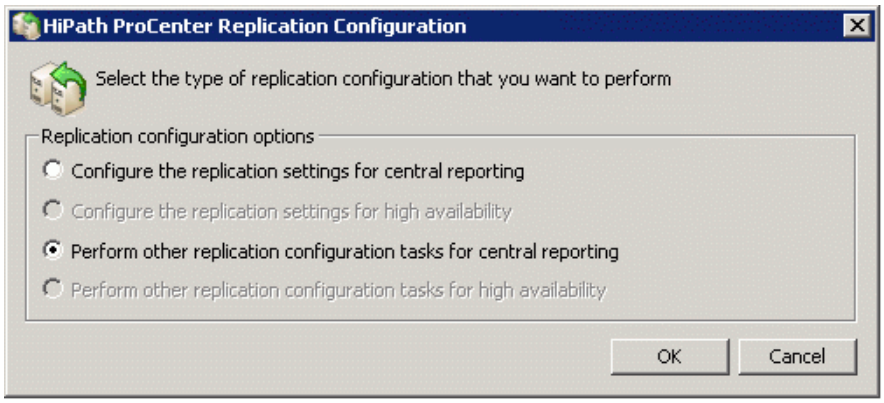
NOTE: Before synchronizing, we recommend that you check the retention periods on the central reporting server machine to ensure that they are not shorter than those configured on the main server machine. If the retention periods are shorter, you might lose some of the synchronized reporting data during the next data maintenance time.

If the system is configured for high availability (warm standby), see Section 8.4, "Synchronizing the reporting data for high availability (warm standby) with central reporting", on page 88.

To synchronize the reporting data:

1. Log on to the central reporting server machine.
2. Stop the **OpenScape Contact Center AutoPA** service on the central reporting server machine. Wait for the service to completely shut down before proceeding.
3. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.

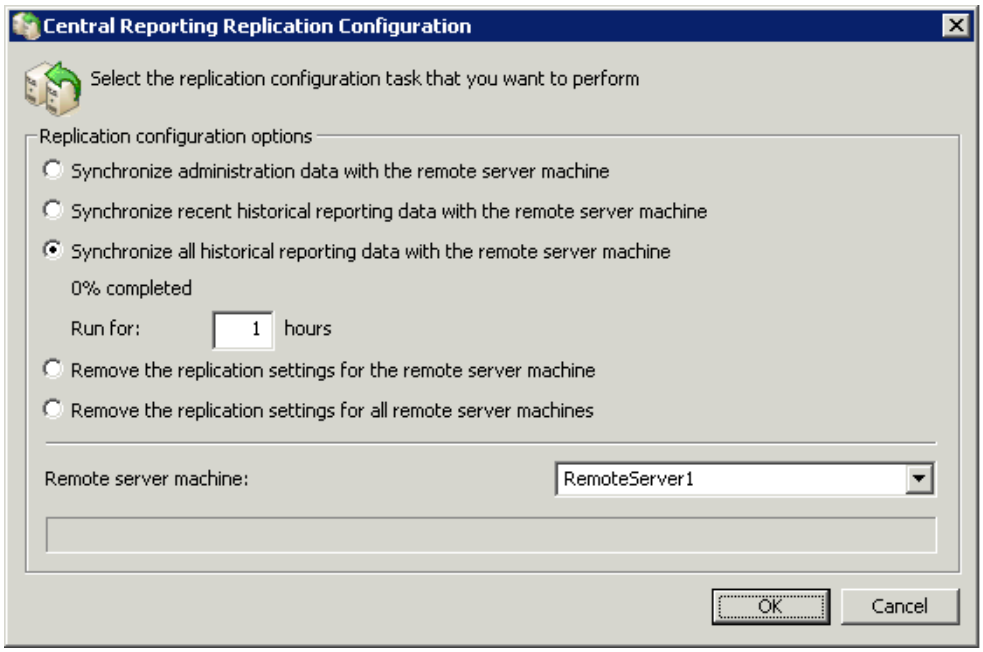
4. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.



5. Select one of the following options, and then click **OK**:

   - To synchronize the historical reporting data for only the current month and the previous month (this option takes less time), do the following:
     - Select **Synchronize recent historical reporting data with the remote server machine**.
     - In the **Remote server** list, select the server machine with which you want to synchronize.
   - To synchronize all historical reporting data, do the following:
     - Select **Synchronize all historical reporting data with the remote server machine**.
     - In the **Remote server** list, select the server machine with which you want to synchronize.
     - Since this option can take a very long time to complete, you can specify how long to run the synchronization. In the **Run for** box, type the number of hours that you want to run the synchronization. After this time period, the synchronization will stop, and you can continue at another time. The % complete value shows how much of the synchronization process is currently complete. The progress bar indicates the progress within the number of hours specified.

- To continue a previous synchronization, select **Continue to synchronize all historical reporting data with the remote server machine**, and then specify the remote server machine and the time to run the synchronization, as described above.



6. When the synchronization is finished, start the **OpenScape Contact Center AutoPA** service on the central reporting server machine.

7.3 Troubleshooting the replication configuration for central reporting

The OpenScape Contact Center replication configuration application (trcdbins.exe) performs a number of tests to ensure that replication has been configured successfully. If you encounter issues with the replication configuration, check the diagnostic files (named trcdbins.000, trcdbins.001... trcdbins.025) that are located in the folder from which you ran the component. These diagnostic files can help you resolve the most common replication configuration issues.

If the diagnostic files do not help you resolve the replication configuration issues, you can perform the troubleshooting procedure described in this section.

You can also use this procedure to troubleshoot central reporting replication configuration issues when the system is configured for high availability (warm standby).

NOTE: This section is written based on the assumption that you are familiar with using Informix. For detailed instructions, see the Informix documentation provided at the following location: http://publib.boulder.ibm.com/infocenter/idshelp/v115/index.jsp

---

To troubleshoot the replication configuration:

1. To check the environment configuration, do the following on the central reporting server machine and each server machine that is participating in central reporting:

   a) On the **Start** menu, point to **Programs**, and then click **Control Panel**.

   b) Double-click **System**.

   c) Click the **Advanced** tab.

   d) Click **Environment Variables**.

   e) Under **System Variables**, ensure that the INFORMIXDIR, INFORMIXSERVER, and ONCONFIG system environment variables appear in the list.

   f) If any of these system environment variables do not appear in the list, add them to the list.

2. Use the `ping` command to ensure that the network connection between the central reporting server machine and each server machine that is participating in central reporting is working properly. If any of the network connections are not working, contact your network administrator.

3. Use the `tracert` command to check the resolution of IP address to host name for the central reporting server machine and each server machine that is participating in central reporting. If any of the IP addresses are not resolved properly to the host names, contact your network administrator.

4. On the central reporting server machine and each server machine that is participating in central reporting, ensure that the hosts.equiv file is located in the `windows\system32\drivers\etc` folder. If the hosts.equiv file does not appear in the folder, ensure that you have write access permissions to the folder.

5. On the central reporting server machine and each server machine that is participating in central reporting, ensure that the hosts.equiv file contains the following lines:

   ```
   <local_host>
   <fully_qualified_local_host_name>
   <remote_host>
   <fully_qualified_remote_host_name
   ```

   where:

   - The fully qualified host names specify the domain, for example, perfect.com.
   - On the central reporting server machine, the remote hosts are the server machines that are participating in central reporting.
   - On a server machine that is participating in central reporting, the remote host is the central reporting server machine.

6. On the central reporting server machine and each server machine that is participating in central reporting, connect to the database servers to ensure that the environment is trusted for the Informix user, as follows:

   a) Log on to the server machine under the **Informix** account.

   b) On the **Start** menu, click **Run**, type **dbaccess**, and then click **OK**.

   c) Select **Connection**.

   d) Select **Connect**.

   e) Select the database server to which you want to connect.

   f) When prompted for the user name, press **ENTER**.

   g) The list of databases on the server should be displayed. If you encounter an error, contact your network administrator. Possible reasons for an error are a DNS lookup problem (forward or reverse DNS lookup table at the Domain Controller) or, when the system is configured for high availability (warm standby), an invalid TCP/IP bindings order for the network interface cards. For high availability (warm standby), the customer network interface card must be at the top of the TCP/IP bindings list, followed by the cluster private network interface card, and then the switch network interface card (if required).

7.4 Replacing a main server machine for central reporting

If a main server machine that is participating in central reporting needs to be replaced, you must follow this procedure.

IMPORTANT: A main server machine should be replaced only under the guidance of your support representative. This procedure does not apply to a central reporting server machine. If you need to replace the central reporting server machine, you must contact your support representative.

NOTE: This procedure requires that you have a backup of all data on the server machine. Ensure that the backup contains the database, registry, and hosts.equiv file. If you do not have a backup of all data on the server machine, then you must also reconfigure the replication settings after performing this procedure. For details, see Section 7.4.1, "Reconfiguring the replication settings", on page 71.

Before you begin, you must obtain a new license file for the new server machine. This is because the System ID used for OpenScape Contact Center licensing is based on the server machine hardware.

To replace a main server machine for central reporting:

1. Restore all data on the new server machine using the most recent backup.
2. Ensure that the patch level of the OpenScape Contact Center server software matches that of the database to be restored.
3. Restore the database on the server machine. For details, follow the procedure provided in Section 6.3.3, "Restoring the database using the ontape utility", on page 52, or Section 6.3.6, "Restoring the database using the onbar utility", on page 55, as appropriate.
4. Using the Manager application, activate the license for the new server machine. For details, see the *Manager Help*.

7.4.1 Reconfiguring the replication settings

If you do not have a backup of all data on the main server machine that needs to be replaced, then you must also reconfigure the replication settings after replacing the server machine.

To reconfigure the replication settings:

1. Remove the replication settings for central reporting:
   - On each of the remaining main server machines that are participating in central reporting (not including the server machine that was replaced), remove the replication settings.
   - On the central reporting server machine, remove the replications settings for all remote server machines.
2. Configure the replication settings.

NOTE: For details on removing and configuring the replication settings, see the *Installation Guide*.

---

8 Managing a high availability (warm standby) environment

This chapter describes the actions that can be taken if you encounter issues when the system is configured for high availability (warm standby).

NOTE: Throughout this chapter, we use the general term "Failover Cluster Manager". If you are using Windows 2012, Windows 2012 R2, Windows 2016, Windows Server 2019 and Windows Server 2022 this refers to the Failover Cluster Management application. For details on the procedures related to these applications, see the Microsoft Help.

8.1 Managing replication for high availability (warm standby)

If there is an issue with replication, the replication buffer will begin to fill up. For details, see Section 7.1.1, "About the replication buffer", on page 59. When this occurs, you can use the OpenScape Contact Center replication configuration application (trcdbins.exe) to manage data replication.

IMPORTANT: The computer clocks on the primary, backup, and optional central reporting server machines must be synchronized. You must synchronize the computer clocks before running the OpenScape Contact Center replication configuration application (trcdbins.exe), and ensure that the clocks remain synchronized. Replication will fail if the times differ by more than two seconds.

8.1.1 Suspending high availability (warm standby) replication

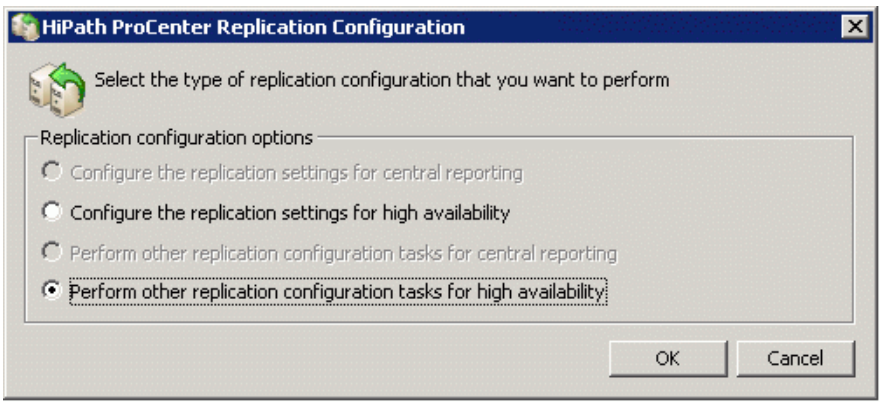
You can suspend the flow of replicated data between the primary and backup server machines, for example, to perform maintenance on the network. We recommend that you suspend replication if you expect the flow of replicated data to be interrupted for more than half a day. It does not matter from which server machine you suspend replication.

This feature is useful because, if a large amount of data accumulates in the buffer during an interruption, significant network and CPU resources will be consumed on the target machine when replication

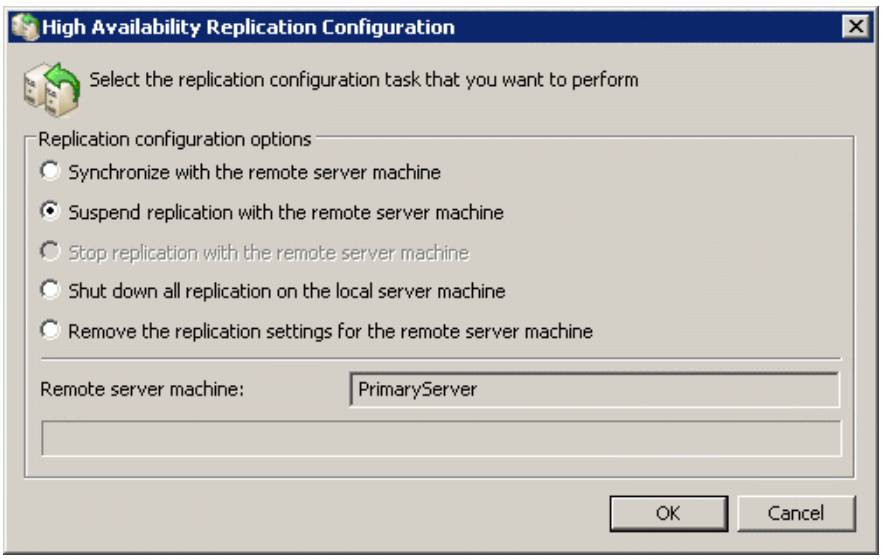
resumes. Suspending replication allows you to resume replication during periods of low contact volume, reducing the impact on the system.

To suspend high availability (warm standby) replication:

1. Log on to either the primary or backup server machine.
2. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
3. Select **Perform other replication configuration tasks for high availability**, and then click **OK**.



4. Select **Suspend replication with the remote server machine**, and then click **OK**.

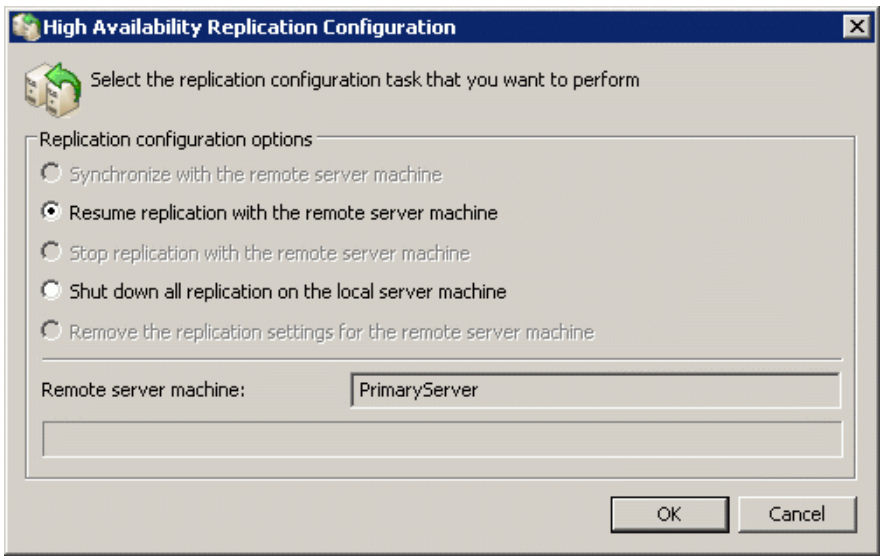


8.1.1.1 Resuming high availability (warm standby) replication

If the replication buffer contains a large amount of data, we recommend that you resume replication during a period of low contact volume to reduce the impact on the system.

To resume high availability (warm standby) replication:

1. Log on to the server machine where you previously suspended replication.
2. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
3. Select **Perform other replication configuration tasks for high availability**, and then click **OK**.
4. Select **Resume replication with the remote server machine**, and then click **OK**.



8.1.2 Suspending central reporting replication

Suspending replication with the central reporting server machine is useful for the reasons described in Section 7.1.2, "Suspending replication for central reporting", on page 60. Follow the procedure described in that section to suspend replication with the central reporting server machine.

NOTE: If the system fails over while central reporting replication is suspended, central reporting replication will restart automatically.

8.1.2.1 Resuming central reporting replication

Follow the procedure described in Section 7.1.2.1, "Resuming central reporting replication", on page 62 to resume replication with the central reporting server machine.

8.1.3 Stopping high availability (warm standby) replication

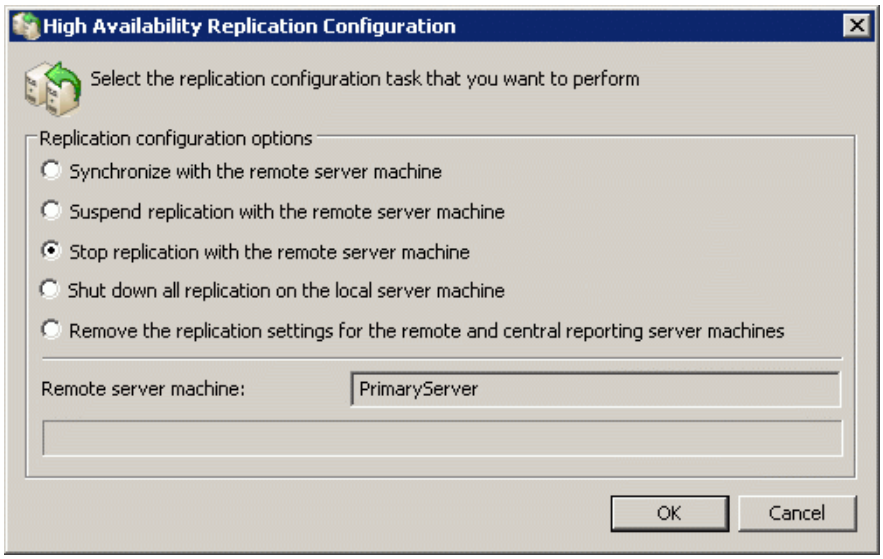
When the system is configured for both high availability (warm standby) and central reporting, you can stop replication between the primary and backup server machines. This allows you to leave central reporting replication running while you address any issues with the network. It does not matter from which server machine you stop replication.

IMPORTANT: You should perform this procedure only when necessary or when instructed to do so because it may require that you synchronize the reporting data. For details, see Section 8.4, "Synchronizing the reporting data for high availability (warm standby) with central reporting", on page 88. Whenever possible, we recommend that you suspend rather than stop replication, because suspending does not require you to synchronize the reporting data.

To stop high availability (warm standby) replication:

1. Log on to the primary or backup server machine.
2. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.

3. Select **Perform other replication configuration tasks for high availability**, and then click **OK**.
4. Select **Stop replication with the remote server machine**, and then click **OK**.



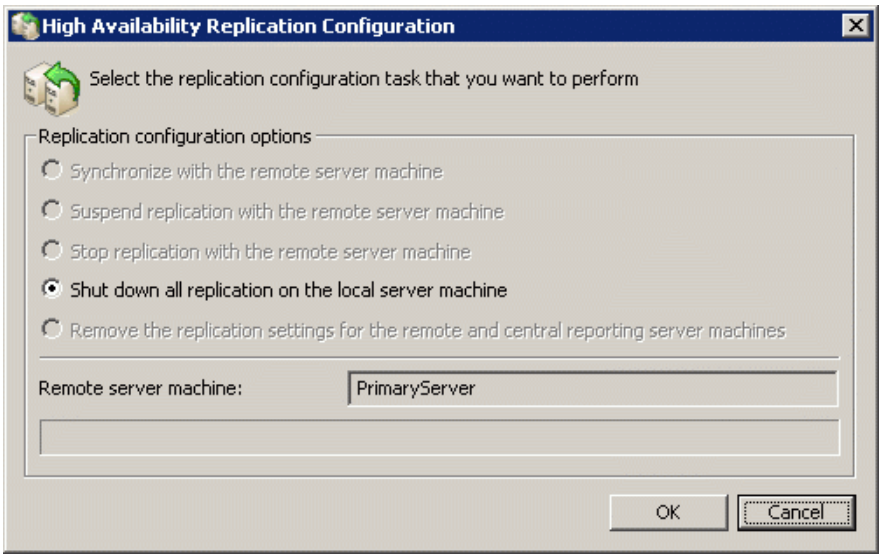
8.1.3.1 Restarting high availability (warm standby) replication

After replication has been stopped, you must first shut down all replication, and then restart replication. During the restart process, all data is removed from the replication buffer.

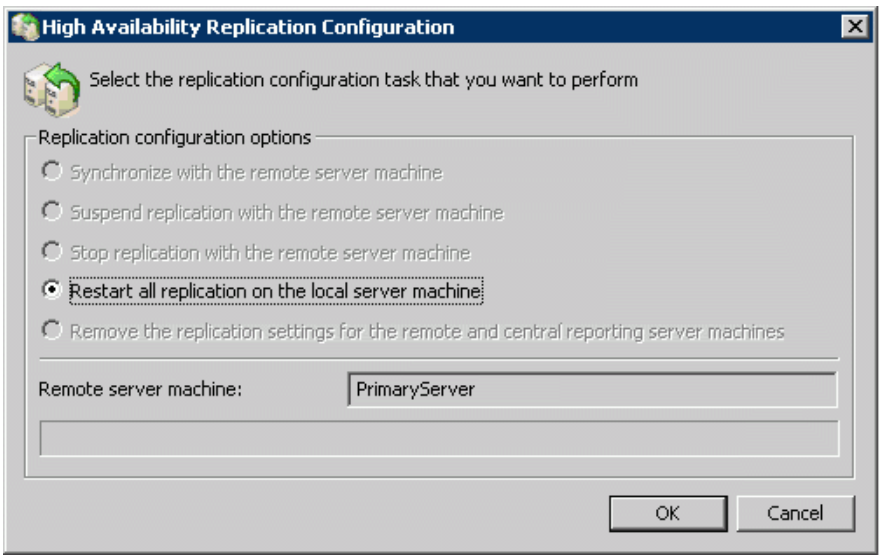
To restart high availability (warm standby) replication:

1. Using the Failover Cluster Manager, take the **HPPC Group** offline. Wait for the server machine state to change to Warm standby before proceeding.
2. Stop the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services on both the primary and backup server machines. Wait for the services to completely shut down before proceeding.
3. Log on to the server machine where you previously stopped replication.
4. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
5. Select **Perform other replication configuration tasks for high availability**, and then click **OK**.

6. Select **Shut down all replication on the local server machine**, and then click **OK**.



7. On the same server machine, run trcdbins.exe again – on the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
8. Select **Perform other replication configuration tasks for high availability**, and then click **OK**.
9. Select **Restart all replication on the local server machine**, and then click **OK**.



10. Synchronize the reporting data, only if required. Section 8.4, “Synchronizing the reporting data for high availability (warm standby) with central reporting”, on page 88.

11. Synchronize the administration data between the primary and backup server machines. For details, see Section 8.2, "Synchronizing the data between the primary and backup server machines", on page 85.
12. If you decided not to synchronize the reporting data in step 10, synchronize the administration data between the primary and central reporting server machine. For details, Section 8.3, "Synchronizing the administration data between the primary and central reporting server machines", on page 87.

8.1.4 Stopping central reporting replication

When the system is configured for both high availability (warm standby) and central reporting, you can stop replication with the central reporting server machine. This allows you to leave high availability (warm standby) replication running while you address any issues with the network or central reporting server machine.

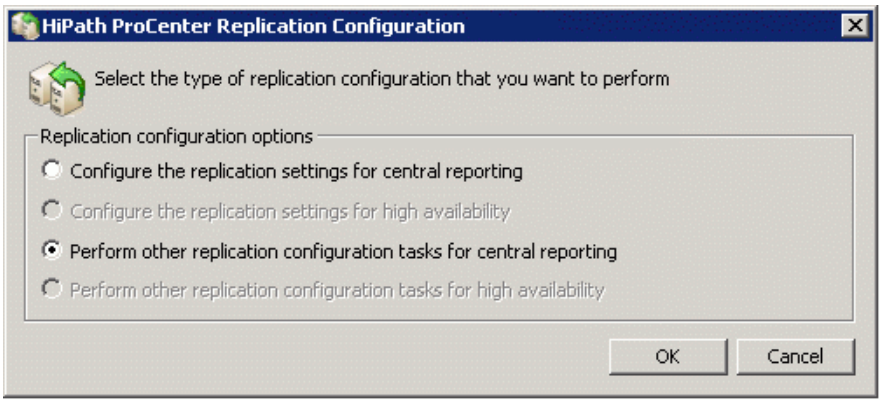
IMPORTANT: You should perform this procedure only when necessary or when instructed to do so because it may require that you synchronize the reporting data. For details, see Section 8.4, "Synchronizing the reporting data for high availability (warm standby) with central reporting", on page 88. Whenever possible, we recommend that you suspend rather than stop replication, because suspending does not require you to synchronize the reporting data.

NOTE: If the system fails over while central reporting replication is stopped, central reporting replication will restart automatically.

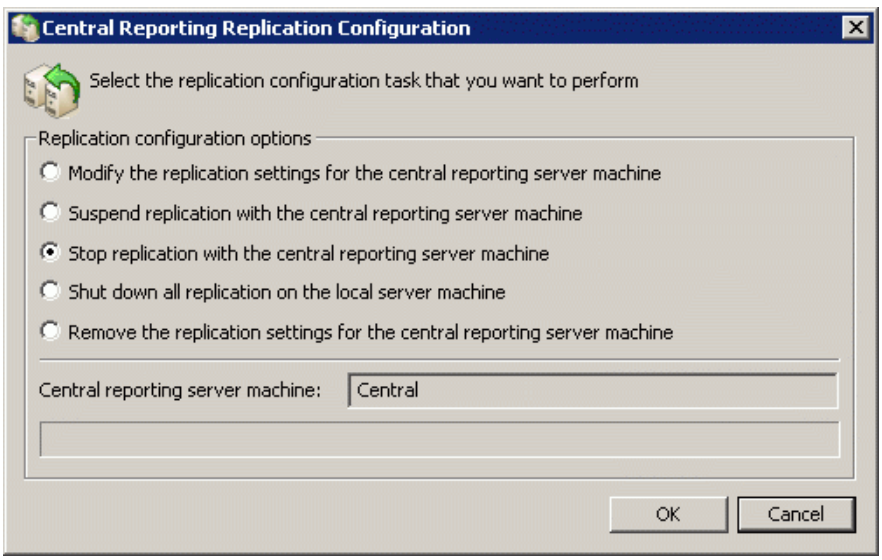
To stop central reporting replication:

1. Log on to the server machine where you want to stop replication with the central reporting server machine.
2. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.

3. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.



4. Select **Stop replication with the central reporting server machine**, and then click **OK**.

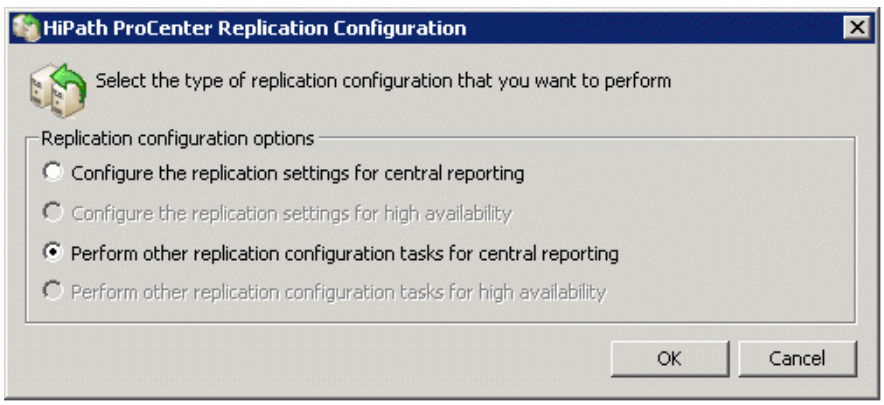


8.1.4.1 Restarting central reporting replication

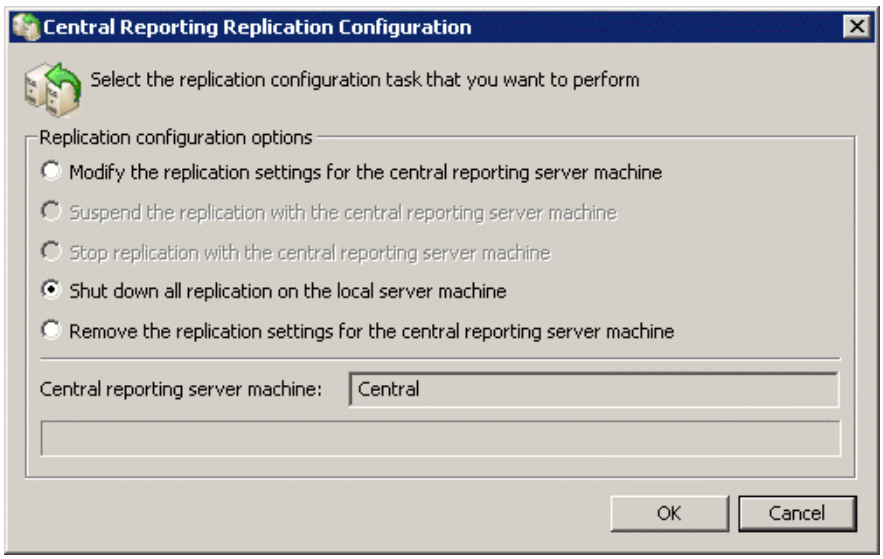
After replication has been stopped, you must first shut down all replication and then restart replication. During the restart process, all data is removed from the replication buffer.

To restart central reporting replication:

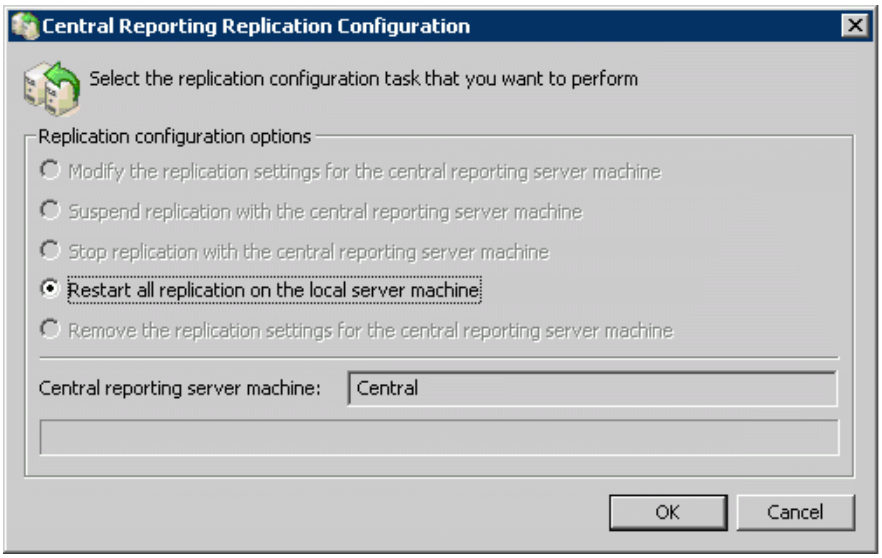
1. Using the Failover Cluster Manager, take the **HPPC Group** offline. Wait for the server machine state to change to Warm standby before proceeding.
2. Stop the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services on both the primary and backup server machines. Wait for the services to completely shut down before proceeding.
3. Log on to the server machine where you previously stopped replication.
4. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
5. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.



6. Select **Shut down all replication on the local server machine**, and then click **OK**.



7. On the same server machine, run trcdbins.exe again – on the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
8. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.
9. Select **Restart all replication on the local server machine**, and then click **OK**.



10. Synchronize the reporting data, only if required. Section 8.4, “Synchronizing the reporting data for high availability (warm standby) with central reporting”, on page 88.
11. Synchronize the administration data between the primary and backup server machines. For details, see Section 8.2, “Synchronizing the data between the primary and backup server machines”, on page 85.
12. If you decided not to synchronize the reporting data in step 10, synchronize the administration data between the primary and central reporting server machine. For details, Section 8.3, “Synchronizing the administration data between the primary and central reporting server machines”, on page 87.

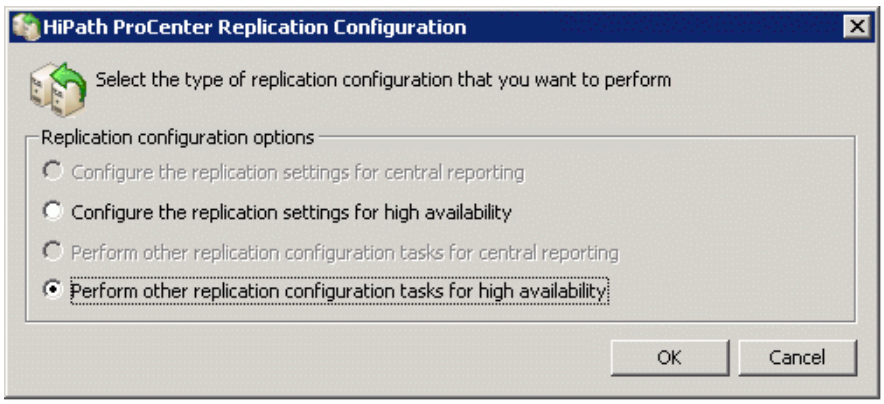
8.1.5 Shutting down all replication

You can shut down all replication on the server machine, for example, if there is an issue with the network and you need to remove the replication settings (which requires network access). When the system is configured for both high availability (warm standby) and central reporting, this shuts down both types of replication.

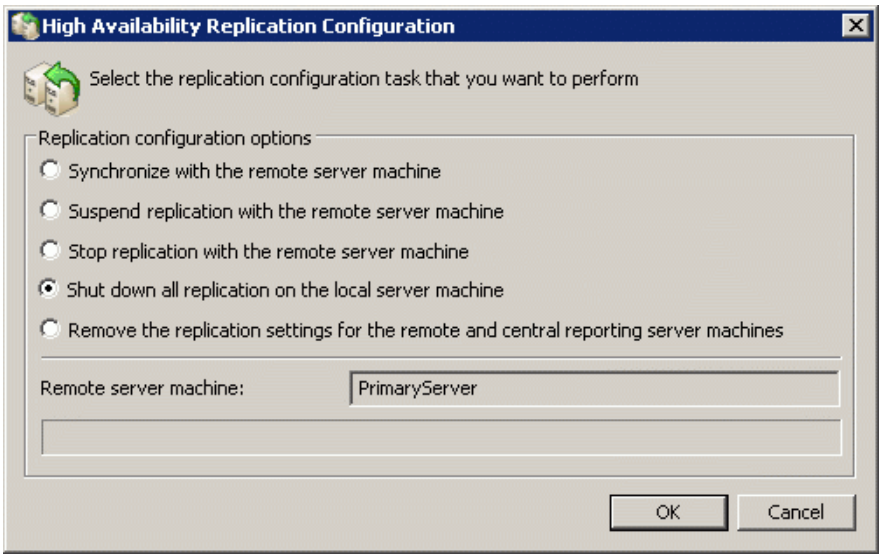
IMPORTANT: You should perform this procedure only when necessary or when instructed to do so because it may require that you synchronize the reporting data. For details, see Section 8.4, "Synchronizing the reporting data for high availability (warm standby) with central reporting", on page 88. Whenever possible, we recommend that you suspend rather than shut down replication, because suspending does not require you to synchronize the reporting data.

To shut down all replication on the server machine:

1. Log on to the server machine where you want to shut down all replication.
2. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
3. Select **Perform other replication configuration tasks for high availability**, and then click **OK**.



4. Select **Shut down all replication on the local server machine**, and then click **OK**.



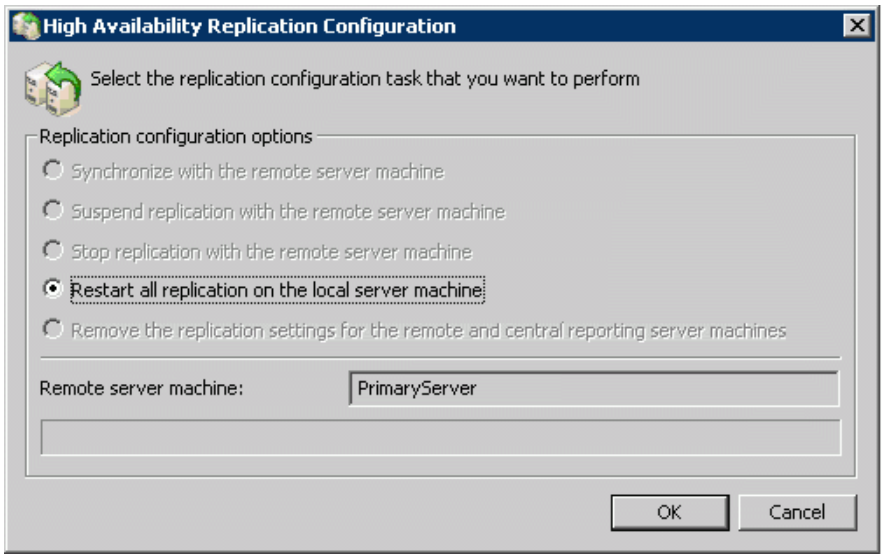
8.1.5.1 Restarting all replication

After all replication on the server machine has been shut down, you can restart it as described in this procedure. When the system is configured for both high availability (warm standby) and central reporting, this procedure restarts both types of replication. During the restart process, all data is removed from the replication buffer.

To restart all replication on the server machine:

1. Using the Failover Cluster Manager, take the **HPPC Group** offline. Wait for the server machine state to change to Warm standby before proceeding.
2. Stop the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services on both the primary and backup server machines. Wait for the services to completely shut down before proceeding.
3. Log on to the server machine where you previously shut down replication.
4. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
5. Select **Perform other replication configuration tasks for high availability**, and then click **OK**.

6. Select **Restart all replication on the local server machine**, and then click **OK**.



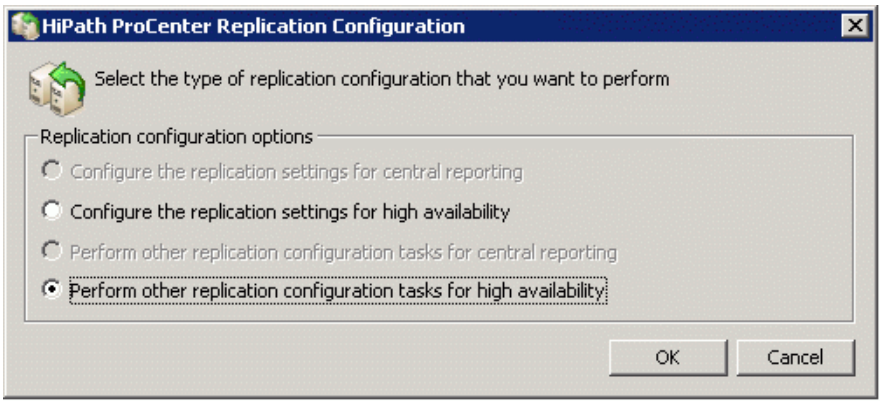
7. Synchronize the reporting data, only if required. Section 8.4, "Synchronizing the reporting data for high availability (warm standby) with central reporting", on page 88.
8. Synchronize the administration data between the primary and backup server machines. For details, see Section 8.2, "Synchronizing the data between the primary and backup server machines", on page 85.
9. If you decided not to synchronize the reporting data in step 7, synchronize the administration data between the primary and central reporting server machine. For details, Section 8.3, "Synchronizing the administration data between the primary and central reporting server machines", on page 87.

8.2 Synchronizing the data between the primary and backup server machines

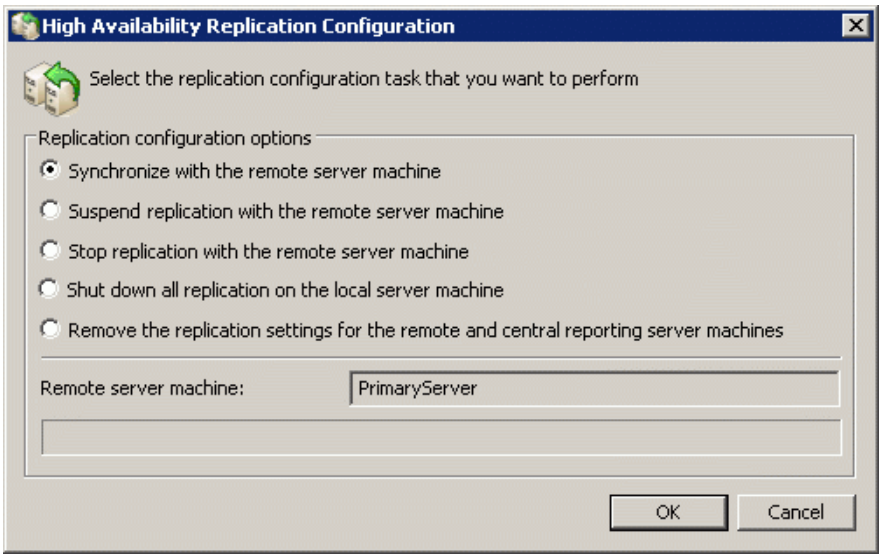
In some cases, you might need to synchronize the administration and processing data between the primary and backup server machines. For example, you might need to perform this procedure if one of the server machines has been down for a long period of time (more than two days), because the system can only buffer a finite amount of data. In this case, you need to perform the procedure on the server machine that has been out of operation and needs to be synchronized.

To synchronize the data between the primary and backup server machines:

1. Using the Failover Cluster Manager, take the **HPPC Group** offline. Wait for the server machine state to change to Warm standby before proceeding.
2. Stop the **OpenScape Contact Center** service on all server machines. Wait for the service to completely shut down before proceeding.
3. Log on to the server machine that needs to be synchronized.
4. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
5. If you have the optional central reporting feature, the OpenScape Contact Center replication configuration options dialog box appears. Select **Perform other replication configuration tasks for high availability**, and then click **OK**.



6. Select **Synchronize with the remote server machine**, and then click **OK**.



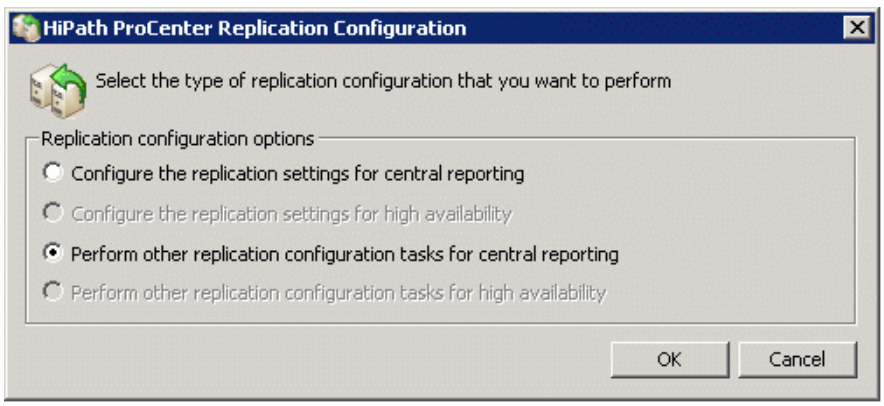
7. When the synchronization is finished, start the **OpenScape Contact Center** service on all server machines.
8. Bring the **HPPC Group** online.

8.3 Synchronizing the administration data between the primary and central reporting server machines

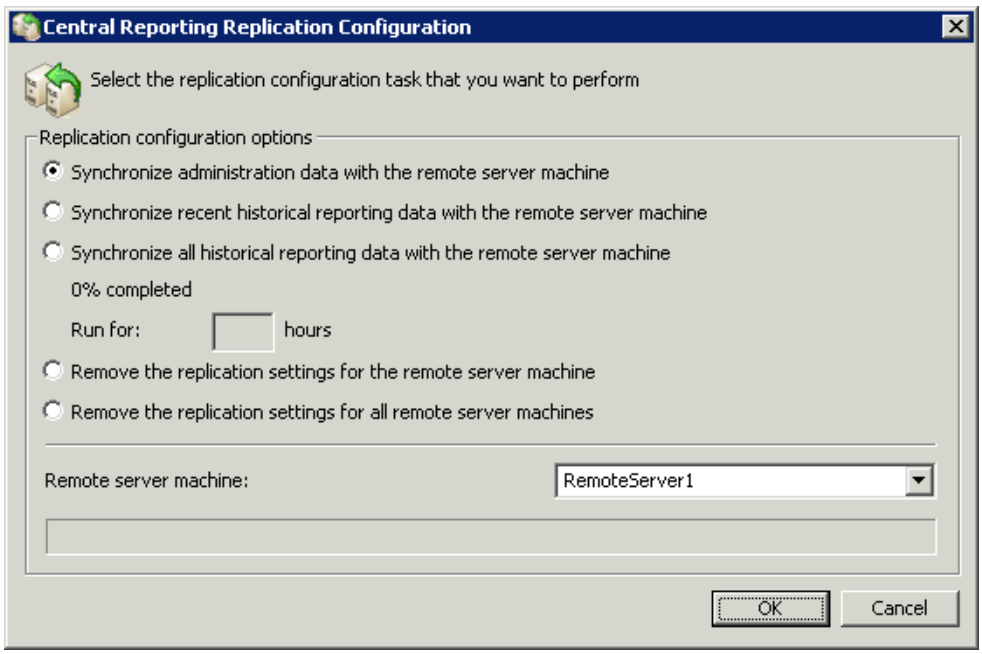
When the system is configured for high availability (warm standby) with central reporting, you might encounter issues that require you to synchronize the administration data between the primary server machine and the central reporting server machine.

To synchronize the administration data between the primary and central reporting server machines:

1. Log on to the central reporting server machine.
2. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
3. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.



4. Select **Synchronize administration data with the remote server machine**, select the primary server machine in the **Remote server machine** list, and then click **OK**.



8.4 Synchronizing the reporting data for high availability (warm standby) with central reporting

If you encounter issues with the historical reporting data, you can synchronize the reporting data. For example, if you are missing data because there has been a lengthy network interruption between one of the main server machines (primary or backup) and the central reporting server machine, you can synchronize the reporting data between the server machine and the central reporting server machine. When you synchronize the reporting data on one server machine in the cluster (primary or backup), you must synchronize the reporting data on the other server machine, as well.

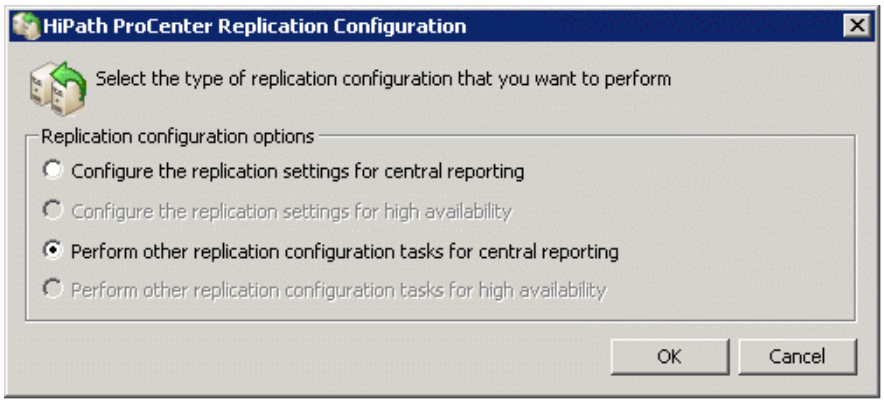
NOTE: Synchronizing the reporting data can take a very long time. We recommend that you perform this procedure only when the issues with the historical reporting data are unacceptable for your purposes.

NOTE: Before synchronizing, we recommend that you check the retention periods on the central reporting server machine to ensure that they are not shorter than those configured on the main server

machine. If the retention periods are shorter, you might lose some reporting data during the first data maintenance time after synchronization.

To synchronize the reporting data for high availability (warm standby) with central reporting:

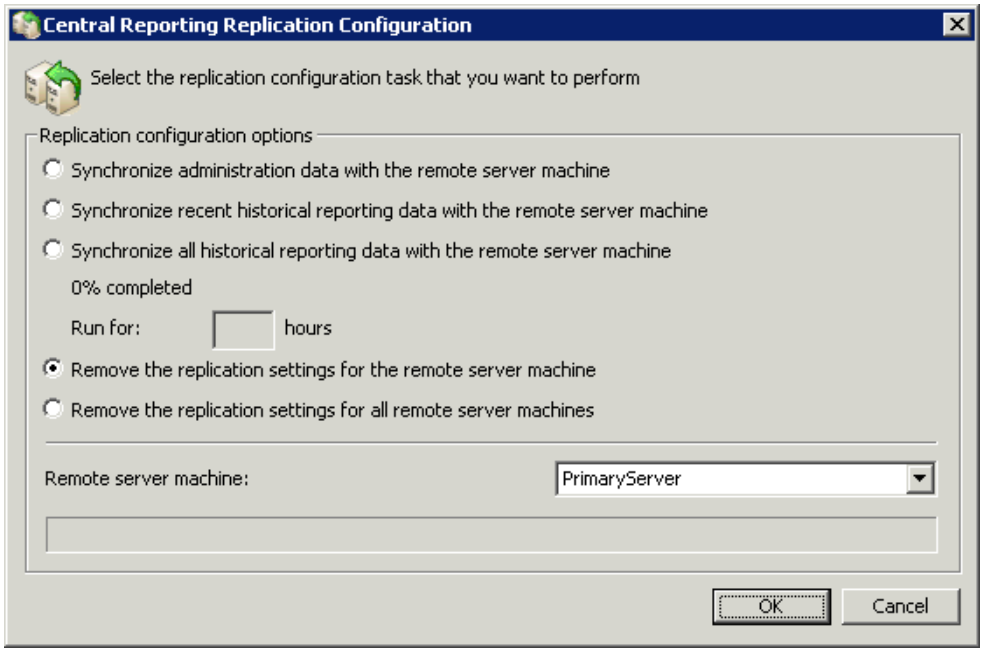
1. Log on to the central reporting server machine.
2. Stop the **OpenScape Contact Center AutoPA** service on the central reporting server machine. Wait for the service to completely shut down before proceeding.
3. On the **Start** menu, click **Run**, type **trcdbins**, and then click **OK**.
4. Select **Perform other replication configuration tasks for central reporting**, and then click **OK**.



5. Select one of the following options, and then click **OK**:
   - To synchronize the historical reporting data for only the current month and the previous month (this option takes less time), do the following:
     - Select **Synchronize recent historical reporting data with the remote server machine**.
     - In the **Remote server** list, select the server machine (primary or backup) with which you want to synchronize.
   - To synchronize all historical reporting data, do the following:
     - Select **Synchronize all historical reporting data with the remote server machine**.
     - In the **Remote server** list, select the server machine (primary or backup) with which you want to synchronize.

  - Since this option can take a very long time to complete, you can specify how long to run the synchronization. In the **Run for** box, type the number of hours that you want to run the synchronization. After this time period, the synchronization will stop, so that you can continue at another time. The % complete value shows how much of the synchronization process is currently complete. The progress bar indicates the progress within the number of hours specified.

- To continue a previous synchronization, select **Continue to synchronize all historical reporting data with the remote server machine**, and then specify the remote server machine (primary or backup) and the time to run the synchronization, as described above.



6. Repeat steps 2 to 5 for the other server machine in the cluster.
7. When the synchronization is finished, start the **OpenScape Contact Center AutoPA** service on the central reporting server machine.

8.5 Troubleshooting the replication configuration for high availability (warm standby)

The OpenScape Contact Center replication configuration application (trcdbins.exe) performs a number of tests to ensure that replication has been configured successfully. If you encounter issues with the replication configuration, check the diagnostic files (named trcdbins.000, trcdbins.001... trcdbins.025) that are located in the folder from which you ran the component. These diagnostic files can help you resolve the most common replication configuration issues.

If the diagnostic files do not help you resolve the replication configuration issues, you can perform the troubleshooting procedure described in Section 7.3, "Troubleshooting the replication configuration for central reporting", on page 68.

8.6 Restoring the database

This section describes how to restore the OpenScape Contact Center database in a high availability (warm standby) environment.

On each server machine where you want to restore the database, you must ensure that:

- The installed OpenScape Contact Center server software is still valid.
- The patch level of the server software matches that of the database to be restored.

If you need to reinstall the OpenScape Contact Center server software or the operating system, you must follow the procedure provided in Section 8.8, "Replacing a server machine in the cluster", on page 95.

8.6.1 Restoring the database on the server machine that is in standby mode

This procedure describes how to restore the OpenScape Contact Center database on the server machine that is in standby mode (normally the backup server machine). Throughout most of this procedure, you can leave OpenScape Contact Center running on the server machine that is in active mode. You only need to stop the OpenScape Contact Center and OpenScape Contact Center AutoPA services for a short time to synchronize the administration data between the primary and backup server machines.

To restore the database on the server machine that is in standby mode:

1. Ensure that the server machine is in standby mode. If the server machine is in active mode, use the Failover Cluster Manager to move the **HPPC Group** to the other server machine.
2. Using the Failover Cluster Manager, pause the server machine.
3. Stop the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services on the server machine that you are restoring. Wait for the services to completely shut down before proceeding.
4. Restore the database on the server machine. For details, follow the procedure provided in Section 6.3.3, "Restoring the database using the ontape utility", on page 52, or Section 6.3.6, "Restoring the database using the onbar utility", on page 55, as appropriate.
5. Synchronize the administration data between the primary and backup server machines. For details, see Section 8.2, "Synchronizing the data between the primary and backup server machines", on page 85.
6. Using the Failover Cluster Manager, resume the server machine.

8.6.2 Restoring the database on the central reporting server machine

This procedure describes how to restore the database on the central reporting server machine only. Throughout most of this procedure, you can leave OpenScape Contact Center running on the server machine that is in active mode. You only need to stop the OpenScape Contact Center and OpenScape Contact Center AutoPA services for a short time after synchronizing the administration data between the primary and central reporting server machines.

When you restore the database on the central reporting server machine, the data will not be synchronized with the primary and backup server machines. You must decide if the reporting data is acceptable for your purposes, or if you want to synchronize the data as described in Section 8.4, "Synchronizing the reporting data for high availability (warm standby) with central reporting", on page 88.

To restore the database on the central reporting server machine:

1. Stop the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services on the central reporting server machine. Wait for the services to completely shut down before proceeding.
2. Restore the database on the server machine. For details, follow the procedure provided in Section 6.3.3, "Restoring the database using the ontape utility", on page 52, or Section 6.3.6, "Restoring the database using the onbar utility", on page 55, as appropriate.
3. Synchronize the reporting data, only if required. For details, see Section 8.4, "Synchronizing the reporting data for high availability (warm standby) with central reporting", on page 88.
4. If you decided not synchronize the reporting data in step 3, you must do the following:
   a) On the server machine that is in active mode (normally the primary server machine), open a command prompt window, type the following, and press **ENTER**:

      ```
      trcdbins -activate
      ```

   b) Synchronize the administration data between the primary and central reporting server machines. For details, see Section 8.3, "Synchronizing the administration data between the primary and central reporting server machines", on page 87.
5. Start the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services on the central reporting server machine.

8.6.3 Restoring the database on more than one server machine

This procedure describes how to restore more than one instance of the OpenScape Contact Center database on the primary, backup, and/or optional central reporting server machine. You must stop the OpenScape Contact Center and OpenScape Contact Center AutoPA services on all server machines for the duration of this procedure.

To restore the OpenScape Contact Center database:

1. Using the Failover Cluster Manager, take the **HPPC Group** offline. Wait for the server machine state to change to Warm standby before proceeding.
2. Stop the **OpenScape Contact Center** and **OpenScape Contact Center AutoPA** services on all server machines. Wait for the services to completely shut down before proceeding.

3. Restore the database on each server machine that needs to be restored. For details, follow the procedure provided in Section 6.3.3, "Restoring the database using the ontape utility", on page 52, or Section 6.3.6, "Restoring the database using the onbar utility", on page 55, as appropriate.
4. Synchronize the administration data between the primary and backup server machines. For details, see Section 8.2, "Synchronizing the data between the primary and backup server machines", on page 85.
5. If the system is configured for central reporting, synchronize the administration data between the primary and central reporting server machine. For details, see Section 8.3, "Synchronizing the administration data between the primary and central reporting server machines", on page 87.

8.7 Forcing a single server machine into service

The OpenScape Contact Center high availability (warm standby) solution uses a majority node set quorum cluster that has two nodes (a primary and a backup server machine) and a file share witness. If both the primary and backup server machines in the cluster become isolated due to a communications failure, a majority cannot be formed and the cluster will lose quorum. This causes the cluster service and OpenScape Contact Center to be terminated. If this occurs, you must manually force quorum on one of the server machines so that the cluster can continue to function.

IMPORTANT: Before you perform this procedure, you must take action to ensure that OpenScape Contact Center cannot become active on both server machines (for example, disconnect the other server machine from the network).

To force a single server machine into service:

1. Use the Service Manager to stop the cluster service on the server machine.
2. Configure the cluster service "start parameters" option as follows:

   `/forcequorum <server machine name>`

   where `<server machine name>` is the name of the server machine.

3. Start the cluster service.

NOTE: Do not click **OK** or **Apply** before starting the cluster service because this will overwrite the start parameters. Also note that the start parameters will not persist after a restart.

8.8 Replacing a server machine in the cluster

If a server machine needs to be replaced, you must follow this procedure to add the new server machine to the cluster.

IMPORTANT: A server machine in the cluster should be replaced only under the guidance of your support representative.

NOTE: This procedure requires that you have a backup of all data on the server machine. Ensure that the backup contains the server machine's System State data, which includes items such as the registry and boot files.

Before you begin, you must:

- Ensure that the new server machine hardware is identical to the server machine hardware that is being replaced. The new server machine must have the same IP address and server name as the server machine that is being replaced.
- Obtain a new license file for the new server machine. This is because the System ID used for OpenScape Contact Center licensing is based on the server machine hardware.

To replace a server machine in the cluster:

1. Restore all data on the new server machine using the most recent backup.
2. Using the Failover Cluster Manager, pause the new server machine.
3. Ensure that the network connections bind to the corresponding network card, and that the network order and the TCP/IP bindings order are correct. The network order is cluster private, customer, and then switch. When configuring the network interface cards, the TCP/IP bindings order is different than the network order. The

customer network interface card must at the top of the TCP/IP bindings list, followed by the cluster private network interface card, and then the switch network interface card (if required).

4. Ensure that the patch level of the OpenScape Contact Center server software matches that of the database to be restored.
5. Restore the OpenScape Contact Center database. For details, see Section 8.6.1, "Restoring the database on the server machine that is in standby mode", on page 91.
6. Using the Manager application, activate the license for the new server machine. For details, see the *Manager Help*.

9 Microsoft Teams deployment

This chapter describes how to configure Microsoft Teams to open up an Agent Portal Lite interface which allows the MS Teams user to control the Routing Status and enable the Preferred Device feature in such a way that an agent can use Teams to receive or make calls via the OSCC Preferred Device feature.

9.1 Editing the tab URL manually

Follow the steps below to edit the tab URL manually:

1. Download the **AgentPortalLite.zip** file which is found in the OpenScape Contact Center Web Components > Microsoft Teams folder from the installed OSCC version.
2. Unzip the **AgentPortalLite.zip** file or directly edit the **manifest.json** file.

   In the **manifest.json** file, edit the **contentUrl** entry by replacing **<appserver>** with your app server (FQDN with valid certificate).

   Save the changes.
3. If needed, zip the files again in the **AgentPortalLite.zip**.

   The files are: **color.png**, **outline.png**, and **manifest.json**.

9.2 Uploading to Microsoft Teams

Follow the steps below to upload the archive to MS Teams:

1. Login to https://admin.teams.microsoft.com/ with an administrator profile account.
2. Navigate to **TeamApps > Manage apps** and click **+ Upload**.
3. Select the **AgentPortalLite.zip** file.

It is also possible to upload directly from MS Teams using an administrator profile account.

1. Login to MS Teams (desktop app or web page) using an administrator account.
2. Navigate to **Apps tab > Manage your apps** and upload the **Agent Portal Lite** app to your organization’s app catalog.

After the upload, you will be able to use the **Agent Portal Lite** app on MS Teams.

Follow the steps below to add the Agent Portal Lite app in MS Teams:

1. Navigate to the apps tab and search for the **Agent Portal Lite** app.
2. Click on the **Agent Portal Lite** app and click **Add**.

NOTE: To have the Agent Portal Lite setup (embedded in the MS Teams), please refer to Agent Portal Lite, User Guide.

---

10 Exchange Calendar Integration

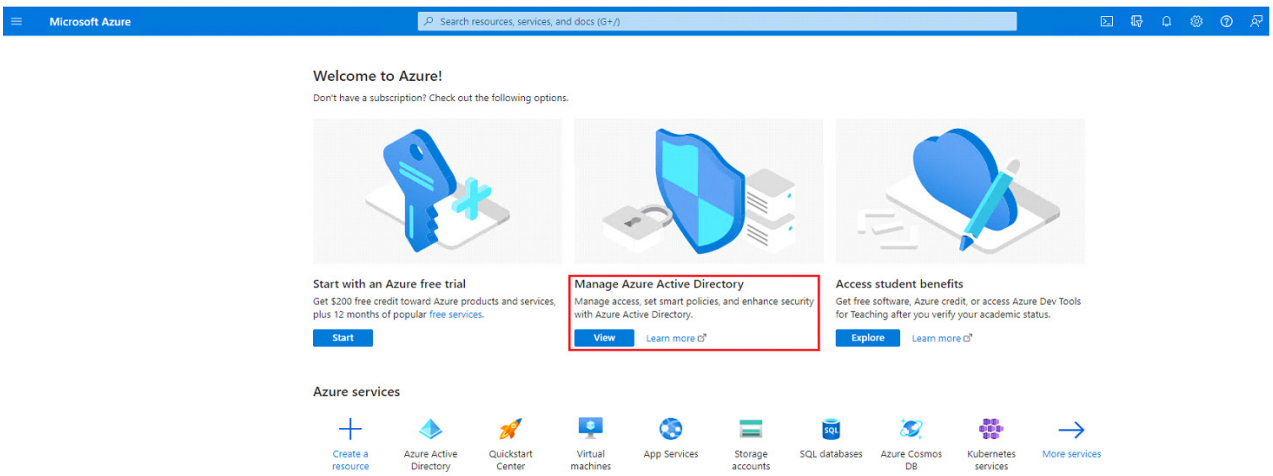
This chapter describes how to configure an Exchange Calendar.

The Exchange Calendar integration provides a way for an agent to see the calendar information of an employee who is in the Speed List or after searching for him/her via the Directory Search. The agent can see the calendar for that person and depending on his/her availability the agent can start a consultation or can schedule a callback, being able to provide an answer straight away to a customer who is calling.

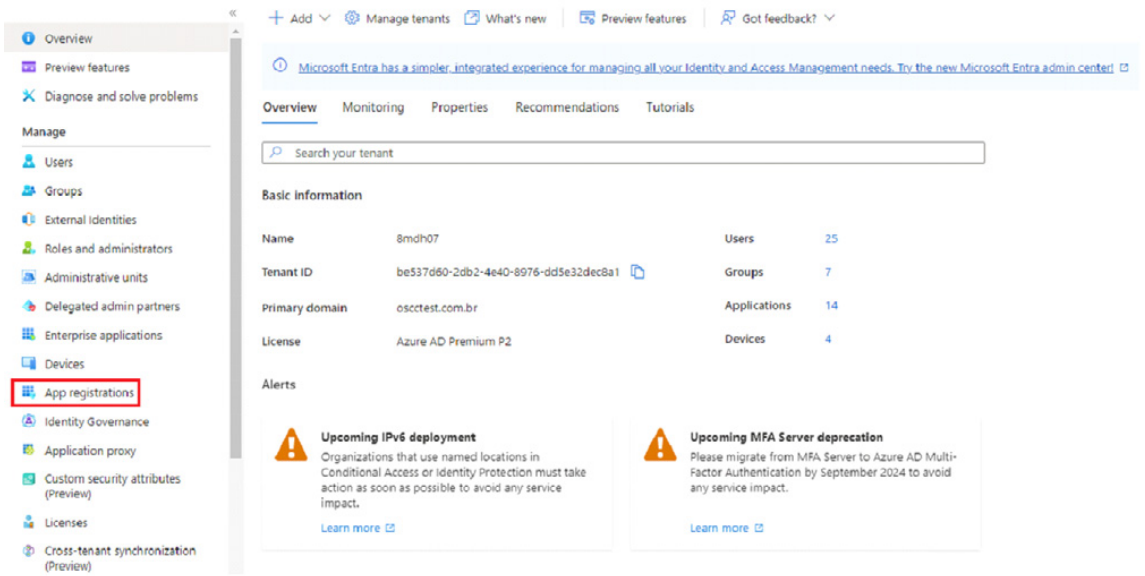
10.1 Azure Configuration

Follow the steps below:

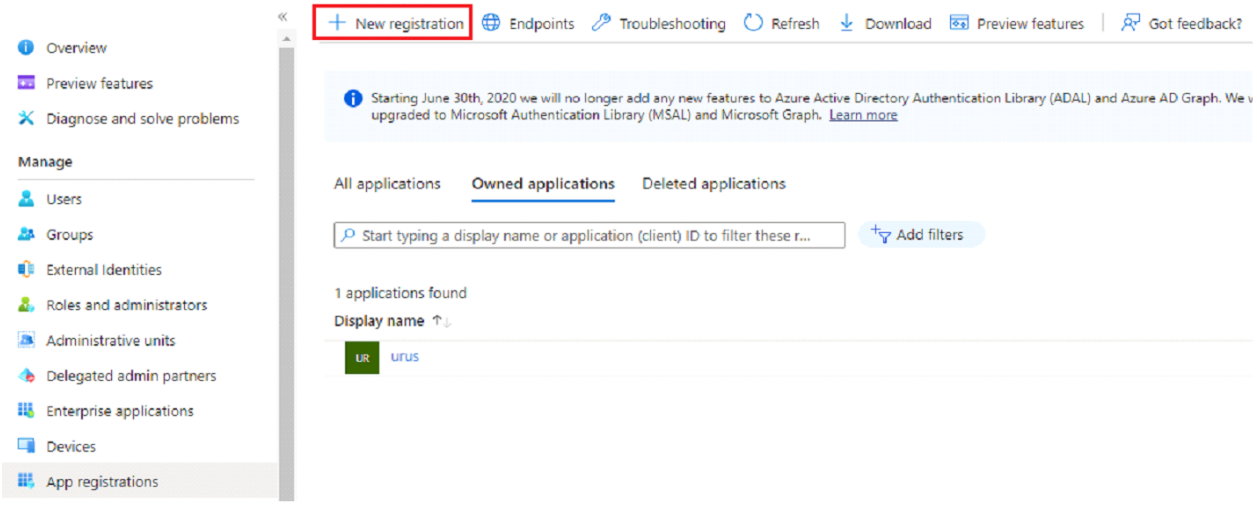
1. Access Azure Portal: https://portal.azure.com/#home
2. Click on **View** at **Manage Azure Active Directory**.



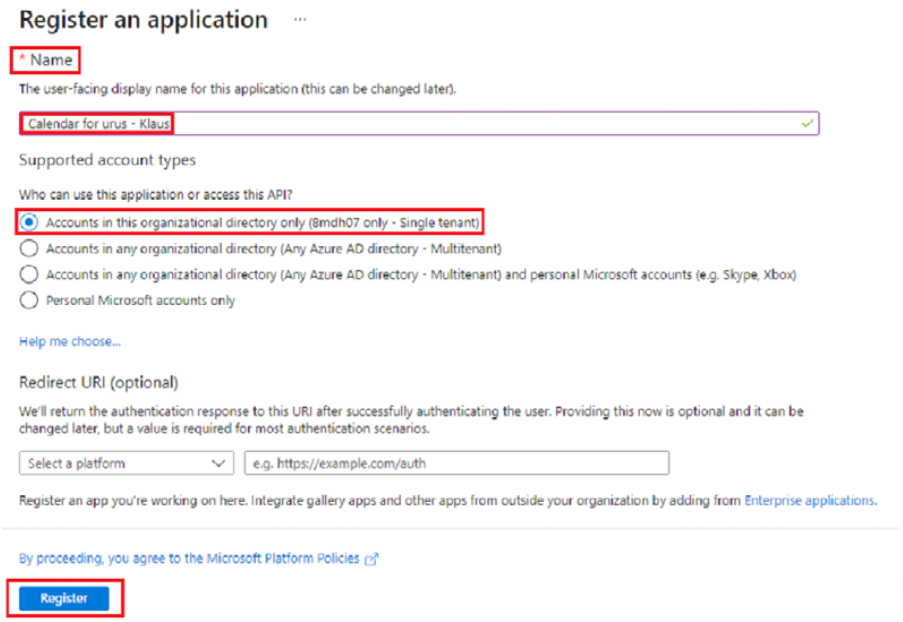
3. Click on **App registrations**



4. Click on **New registration**

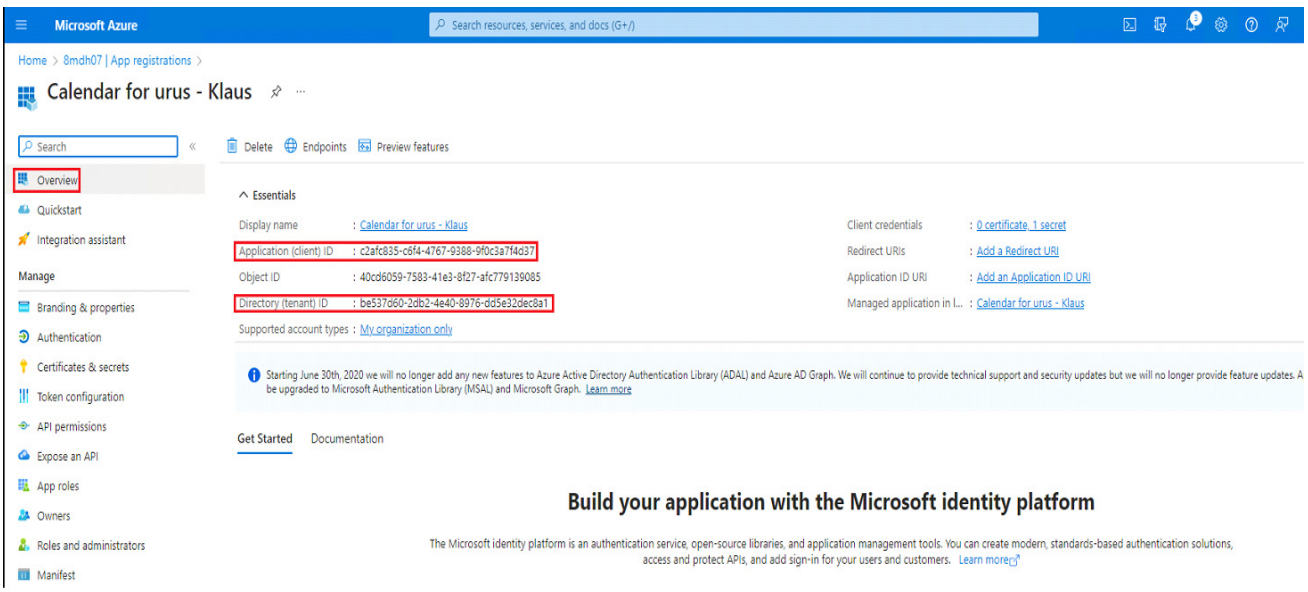


5. Enter **Name**, select **Accounts in this organizational directory (<domain name> - Single Tenant)** and then, click on **Register**.

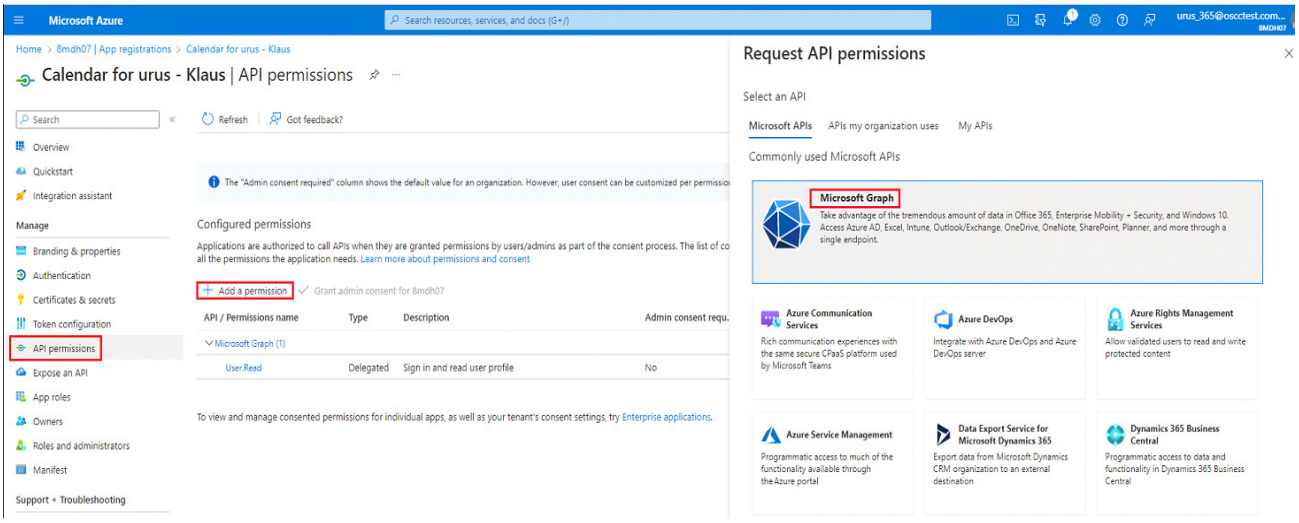


6. Copy and Save the **Application (client) ID and Directory (tenant) ID**.

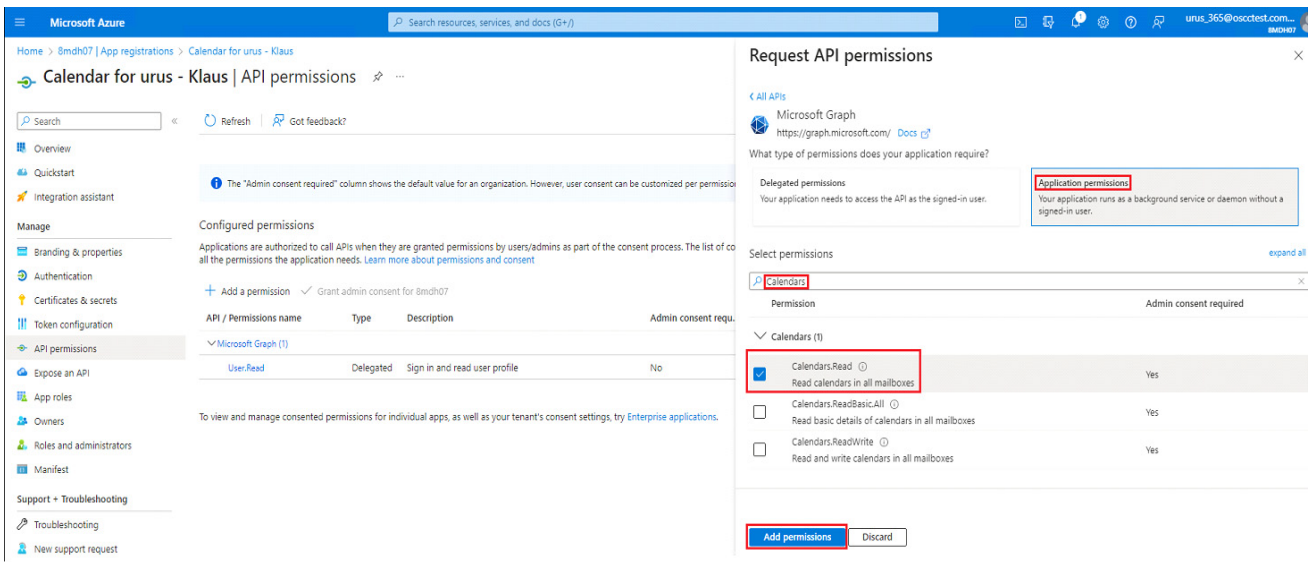
   This information can be copied later from the option **Overview**.



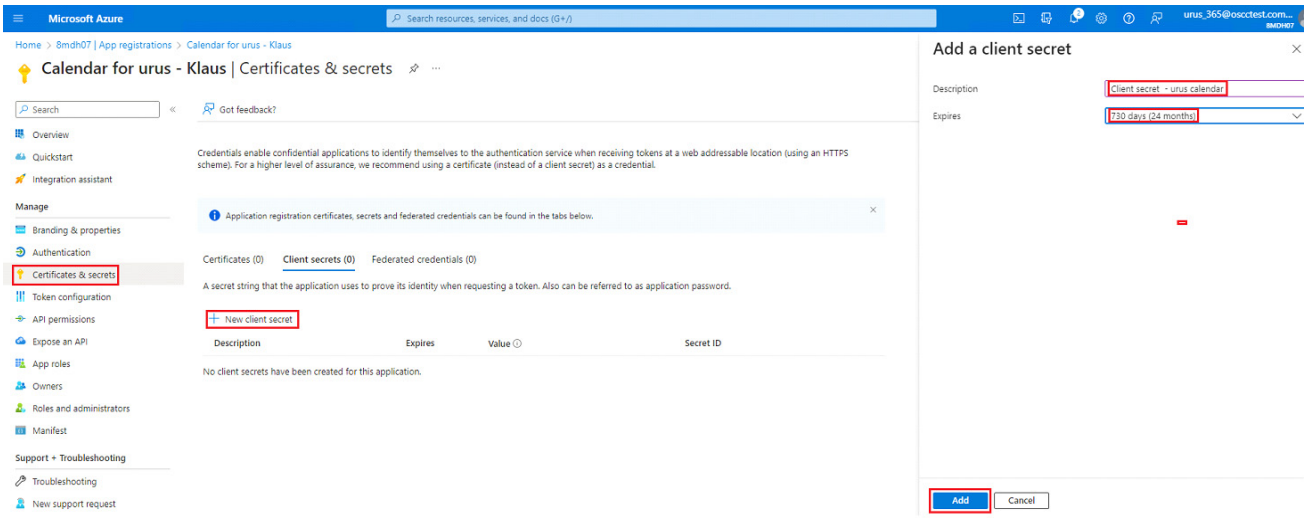
7. Click on **API permissions**, then on Add a permission and on **Microsoft Graph**:



8. Click on **Application permission**, select the option **Calendars.Read** (use the search option to facilitate) and click on **Add permission**.

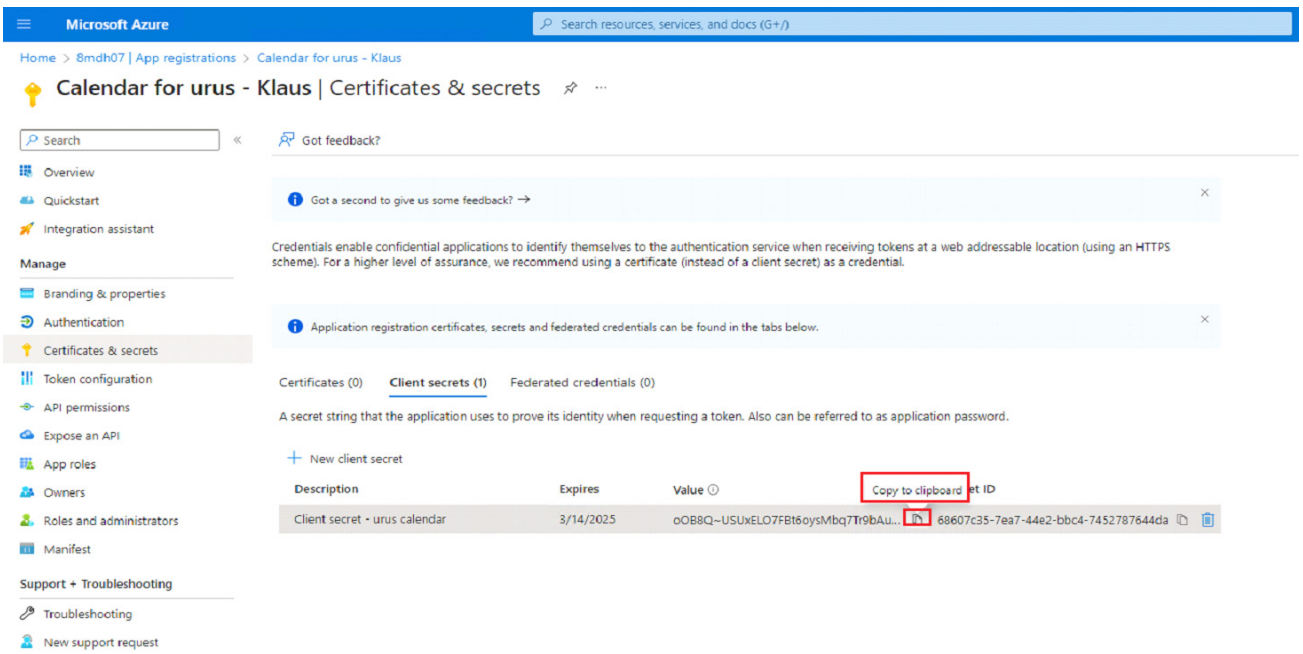


9. Click on **Certificates & secrets**, **New client secret**, enter a **Description**, select when it **Expires** and click on **Add**.



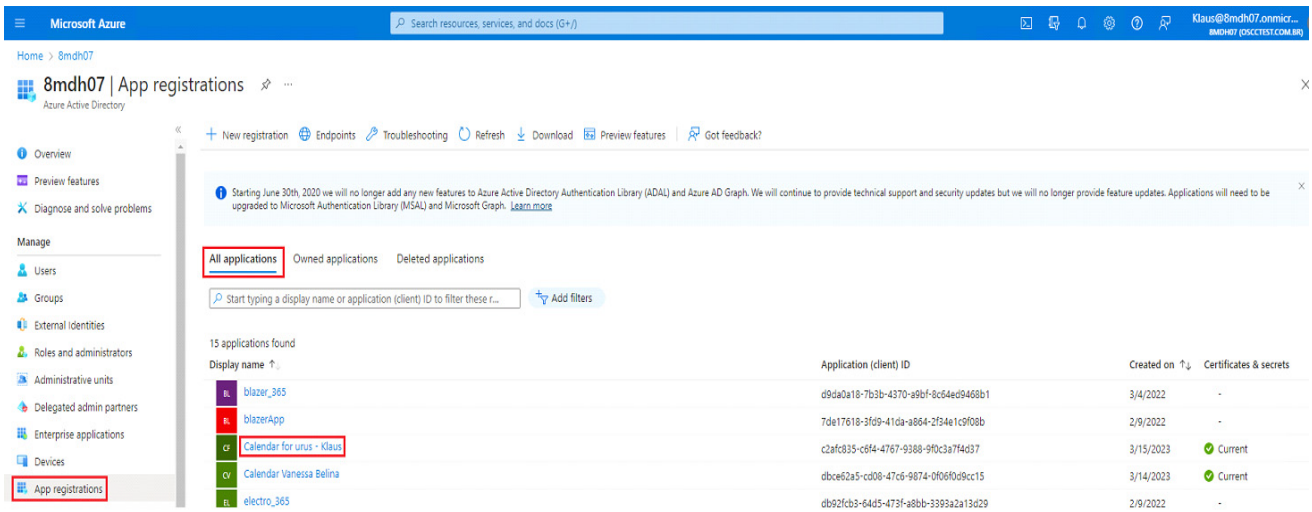
10. Copy this client secret Value and save it.

NOTE: It is very important to execute this step at this point because: ***Client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving the page.***

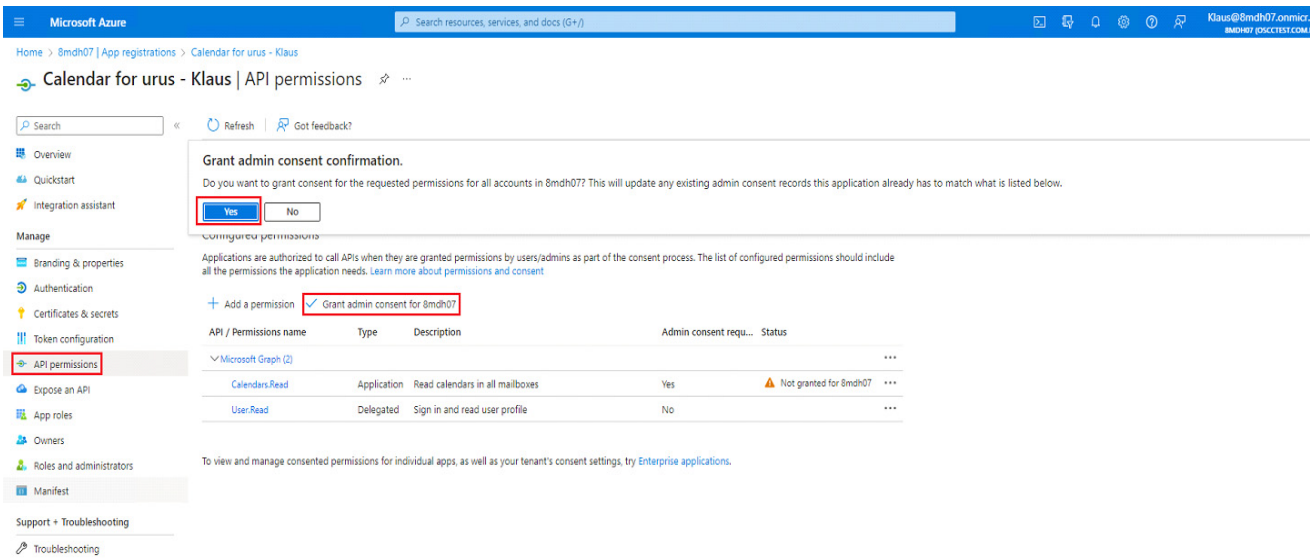


11. Sign out Azure portal, login with administration account.

Click on: **Manager Azure Active Directory ->View ->App registrations -> All applications** and the **created application**.



12. Click on **API permissions -> Grant admin consent for the <domain>”**



After this configuration is done, you need to configure it at the Web Manager side.

Please refer to *Web Manager Administration Guide*, section *Exchange Calendar Integration* to complete the Exchange Calendar configuration.

NOTE: Multitenant environment accepts the configuration only from one Azure domain per tenant.

Index

A

administration data
- synchronizing for high availability (warm standby) with central reporting 87

Apache Tomcat version 21
authentication, e-mail server 19

B

backups, see database backups

C

central reporting
- about the replication buffer 59
- managing the replication 59
- replacing a main server machine 71
- restarting the replication 65
- resuming the replication 62
- shutting down the replication 63
- suspending the replication 60
- synchronizing server machine clocks 59
- synchronizing the reporting data 66
- troubleshooting the replication configuration 68

config.properties
- configuring on a Sun Java System Web Server 32
- configuring on a Tomcat server 28

corporate e-mail server
- configuring 11
- requirements 11
- setting up a secure connection 18
- using authentication 19

corporate Web server
- Apache Tomcat version 21
- configuring 21, 22
- customized files and upgrading 21
- requirements 21
- setting up a secure connection 34
- Sun Java System version 21
- supported operating systems 21

custom e-mail message headers
- about 12
- inserting 15

D

data replication, see replication
database backups
- full backups 48
- incremental backups 48
- restoring using onbar utility 55
- restoring using ontape utility 52
- scheduling 49
- to a local drive (onbar) 54
- to a local or network drive (ontape) 51
- to a local tape drive (ontape) 50

documentation
- formatting conventions 7, 97
- intended audience 7
- providing feedback 8

E

e-mail message headers
- custom required 12
- inserting custom 15

e-mail reports feature, support for 19
e-mail server 11
- setting up a secure connection 18
- using authentication 19

error codes, for Web callback 42

F

Failover Cluster Management application 73

H

high availability (warm standby)
- about the replication buffer 59
- forcing quorum on a single server machine 94
- managing the replication 73
- replacing a server machine in the cluster 95
- restarting all replication 84
- restarting the central reporting replication after stopping 80
- restarting the replication after stopping 77
- restoring the database 91
- resuming the central reporting replication 76
- resuming the replication 75
- shutting down all replication 83
- stopping the central reporting replication 79
- stopping the replication 76
- suspending the central reporting replication 76
- suspending the replication 73
- synchronizing administration data for central reporting 87
- synchronizing server machine clocks 73
- synchronizing the data 85
- synchronizing the reporting data 88

TCP/IP bindings order 95
troubleshooting the replication configuration 91
HPWC.ini file
configuring 24
enabling for SSL 35
troubleshooting issues 40, 41

I

IBM Lotus Domino deployment 16
IIS server
configuring the HPWC.ini file 24
configuring Web components 23
creating a virtual directory 24
setting up a secure connection 35
testing VoiceXML integration 26
testing Web callback 26
testing Web collaboration 25
IMAP4 protocol 11
Informix
changing the password 46
configuring the ontape parameters 49, 51
using the onbar utility 54
using the ontape utility 50
IP connections, configuring for wallboards 9
ISAPI extensions 24

J

Java Runtime Engine 41
JSSE library 41

L

LDAP directory, configuring for presence integration 44
localizing Web components 37
Lotus Domino deployment 16

M

Microsoft Cluster Administrator application 73
Microsoft Exchange deployment 14
MIME functions 11

O

OpenScape Contact Center password, changing 46
OpenScape UC Application user account, configuring for presence integration 43

P

passwords, changing 46
presence integration, configuring 43

Q

quorum, forcing on a single server machine 94

R

remote service access 45
replication
managing for central reporting 59
managing for high availability (warm standby) 73
restarting after stopping for high availability (warm standby) 77
restarting all replication 84
restarting for central reporting 65
restarting for central reporting after stopping 80
resuming for central reporting 62
resuming for high availability (warm standby) 75
shutting down all replication 83
shutting down for central reporting 63
stopping for central reporting 79
stopping for high availability (warm standby) 76
suspending for central reporting 60
suspending for high availability (warm standby) 73
troubleshooting for central reporting 68
troubleshooting for high availability (warm standby) 91
reporting data
synchronizing for central reporting 66
synchronizing for high availability (warm standby) with central reporting 88

S

scheduled backups 49
secure connection
for a corporate e-mail server 18
for a corporate Web server 34
server machine, shutting down for maintenance 45
SMTP protocol 11
SNMP support, methods 55
SSDP Service Plug-in 45
SSL
enabling for a corporate e-mail server 18
enabling for a corporate Web server 34
enabling on a Sun Java server 36
enabling on a Tomcat server 36
enabling on an IIS server 35
troubleshooting 41
Sun Java System Web Server
configuring and deploying the .war file 31
configuring Web components 31
editing config.properties 32
setting up a secure connection 36
testing Web callback 34
testing Web collaboration 33
Sun Java System Web Server version 21
synchronizing
administration and processing data for high availability (warm standby) 85

administration data for high availability (warm standby) with central reporting 87
reporting data for central reporting 66
reporting data for high availability (warm standby) 88

T

Tomcat server
configuring and deploying the .war file 27
configuring Web components 27
editing config.properties 28
setting up a secure connection 36
testing VoiceXML integration 30
testing Web callback 30
testing Web collaboration 29
troubleshooting
configuring Web server 40
HPWC.ini file 40, 41
replication configuration for central reporting 68
replication configuration for high availability (warm standby) 91
SSL 41
Web collaboration 40

U

utilities
osccmseheaders 15
utilties
osccregistersnmpextension 57

V

virtual directory, IIS server 24
VoiceXML integration
testing on a Tomcat server 30
testing on an IIS server 26

W

wallboards, configuring 9
.war file
configuring on Tomcat server 27
configuring on a Sun Java System Web Server 31
Web browser requirements 21
Web callback
error codes 42
testing on a Tomcat server 30
testing on an IIS server 26
testing on Sun Java server 34
Web collaboration
testing on IIS server 25
testing on Sun Java server 33
testing on Tomcat server 29
troubleshooting 40
Web components
configuring 22
configuring on a Sun Java server 31
configuring on a Tomcat server 27
configuring on an IIS server 23
customizing 38
localizing 37
setting up a secure connection 34
system requirements 21
Web browser requirements 21
Web server
Apache Tomcat version 21
configuring 21, 22
customized files and upgrading 21
requirements 21
setting up a secure connection 34
Sun Java System version 21
supported operating systems 21
troubleshooting 40