A MITEL
PRODUCT
GUIDE

Mitel OpenScape Contact Center Agile V12

System Management Guide V12

System Management Guide

Service Documentation
10/2024

A31003-S22C0-S103-01-7620

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 . . . 5
1.1 Who should use this guide . . . 5
1.2 Formatting conventions . . . 5
1.3 Documentation feedback . . . 6
2 Configuring a wallboard . . . 7
2.1 Before you begin . . . 7
2.2 Configuring the IP connection for a wallboard . . . 7
3 Configuring the corporate e-mail server . . . 9
3.1 Corporate e-mail server requirements . . . 9
3.2 Planning the Microsoft Office 365 deployment . . . 10
3.3 Planning the Google GSuite deployment . . . 11
3.4 Planning the Microsoft Exchange deployment . . . 12
3.4.1 Specifying custom headers (Microsoft Exchange Server 2007, 2010, and 2013 only) . . . 13
3.5 Planning the IBM Lotus Domino deployment . . . 14
3.5.1 Compacting the database . . . 15
3.6 Setting up a secure connection for an e-mail server . . . 16
3.7 Using authentication on an e-mail server . . . 17
3.8 Supporting the e-mail reports feature . . . 17
4 Configuring the corporate Web server . . . 19
4.1 System requirements for using Web components . . . 19
4.1.1 Corporate Web server requirements . . . 19
4.1.2 Web browser requirements . . . 19
4.2 Configuring Web components . . . 20
4.2.1 Configuring an IIS server . . . 20
4.2.1.1 Configuring the Web component files on an IIS server . . . 21
4.2.1.2 Testing Web callback on an IIS server . . . 23
4.2.2 Configuring a Tomcat server . . . 23
4.2.2.1 Configuring the .war file on a Tomcat server . . . 24
4.2.2.2 Testing Web callback on a Tomcat server . . . 25
4.2.3 Configuring a Sun Java System Web Server . . . 25
4.2.3.1 Configuring the .war file on a Sun Java System Web Server . . . 26
4.2.3.2 Testing Web callback on a Sun Java System Web Server . . . 27
4.3 Setting up a secure connection for a Web server . . . 28
4.3.1 Enabling TLS on an IIS server . . . 29
4.3.2 Enabling TLS on a Tomcat or Sun Java server . . . 29
4.4 Web callback error codes . . . 30
5 Configuring the presence integration . . . 33
5.1 Configuring an OpenScape UC Application user account . . . 33
5.2 Configuring the external LDAP directory . . . 34
6 Maintaining the system . . . 35
6.1 Shutting down a server machine for system maintenance . . . 35
6.2 Changing the OpenScape Contact Center and Informix passwords . . . 36
6.3 Backing up the database . . . 38
6.3.1 Scheduling a database backup . . . 39
6.3.2 Backing up the database using the ontape utility . . . 40

6.3.2.1 Backing up the database to a local tape drive 40
6.3.2.2 Backing up the database to a local or network drive 41
6.3.3 Restoring the database using the ontape utility 42
6.3.4 Restoring a zero level backup made using ontape utility 43
6.3.5 Backing up the database using the onbar utility 44
6.3.6 Restoring the database using the onbar utility 45
6.4 SNMP support 45
6.4.1 OpenScape Contact Center SNMP extension agent 46
6.4.2 OpenScape CAP Fault Management software 47

7 Microsoft Teams deployment 49
7.1 Editing the tab URL manually 49
7.2 Uploading to Microsoft Teams 49

8 Exchange Calendar Integration 51
8.1 Azure Configuration 51

Index 58

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 Agile V12 system. It also describes how to perform ongoing maintenance of the Unify OpenScape Contact Center Agile 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 Agile V12 system.

1.2 Formatting conventions

The following formatting conventions are used in this guide:

Bold
This font identifies Unify OpenScape Contact Center Agile 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-S103-01-7620

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:

- **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 ensures that if a customer sends an e-mail message to an alias, such as sales@company.com, it can be routed appropriately. 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 callback feature. 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. For details, see Section 4.3, "Setting up a secure connection for a Web server", on page 28.

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 **HPPCAgileWeb.zip** file to the corporate Web server machine and unzip the file to the folder 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\english (and corresponding files)

   c:\HPPC\images (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.

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 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*.

4.2.2 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 **HPPCAgileWeb.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: 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 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*.

4.2.3 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 **HPPCAgileWeb.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: 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 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 26.

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.
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 callback flag to true:

   ```
   CallbackUsesSSL=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.
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 callback flag to true:

   ```
   socket.webcallback.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 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.

Table 1 Web Callback Error Codes

Error Code	Description
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 1 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.

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)

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 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”.

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.

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 41.

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.
- **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.

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

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.

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 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.

7.1 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**.

7.2 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.

---

8 Exchange Calendar Integration

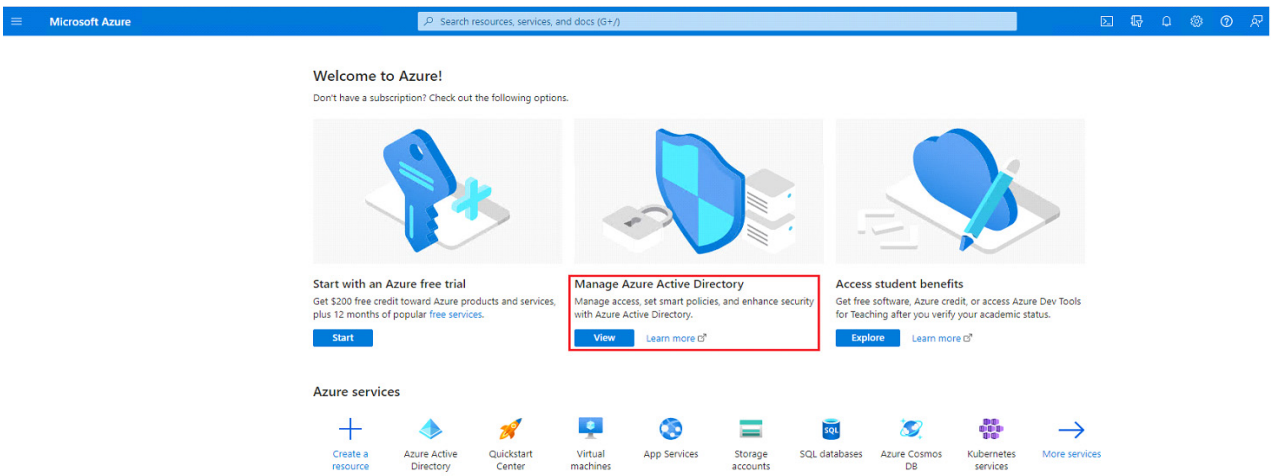
This chapter describes how to configure an Exchange Calendar.

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.

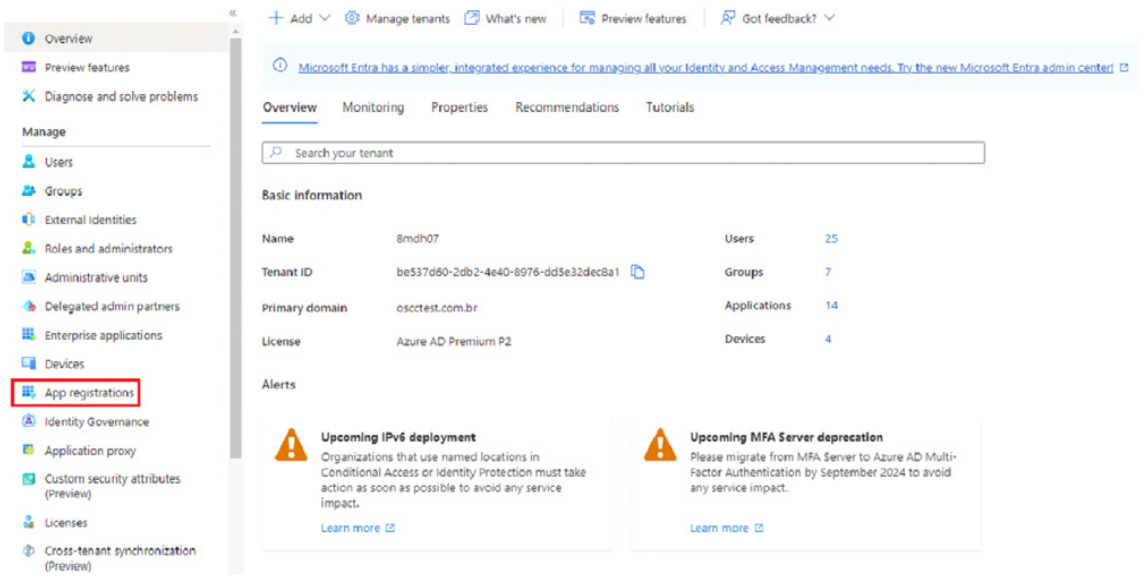
8.1 Azure Configuration

Follow the steps below:

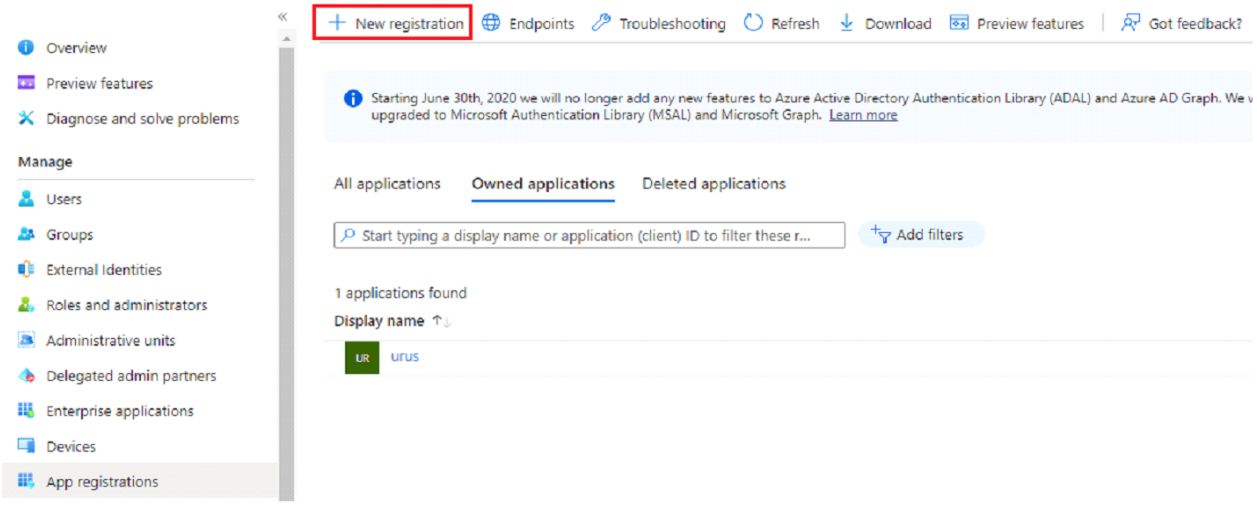
1. Access Azure Portal: https://portal.azure.com/#home
2. Click on **View** at **Manage Azure Active Directory**.



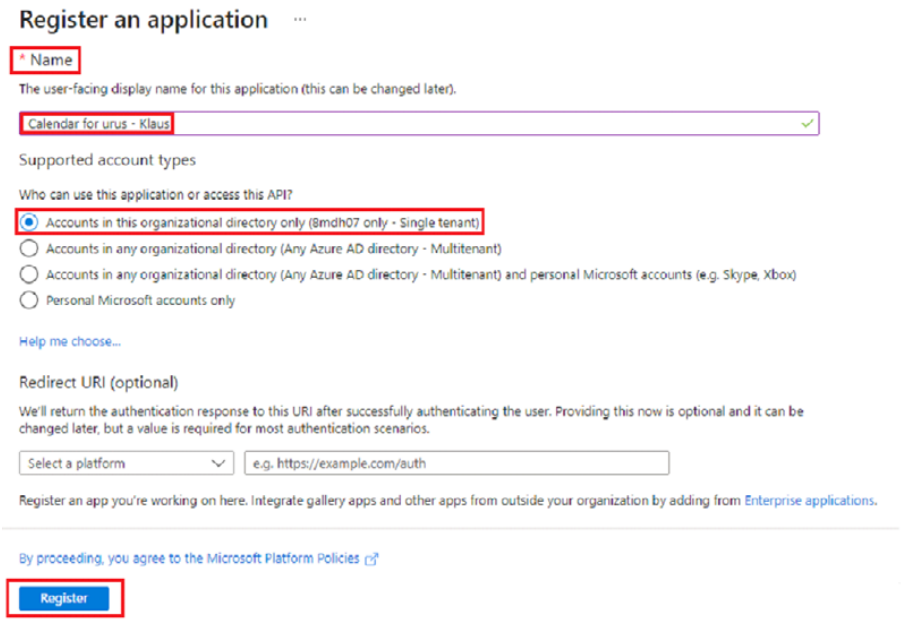
3. Click on **App registrations**



4. Click on **New registration**

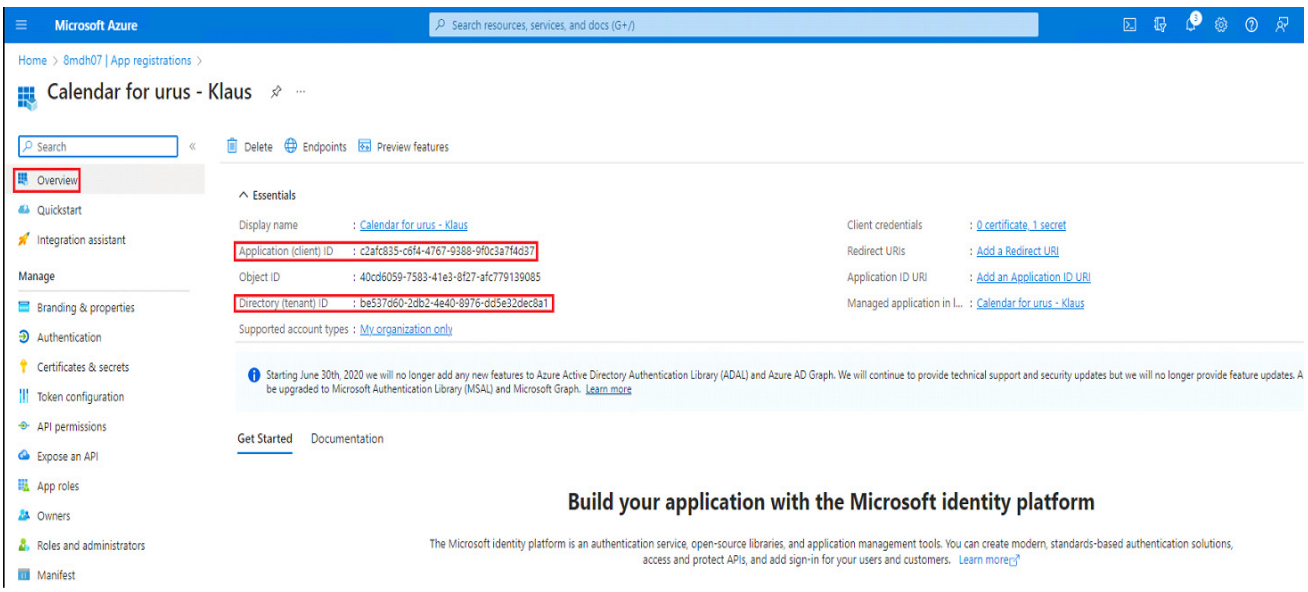


5. Enter **Name**, select **Accounts in this organizational directory (<domain name> - Single Tenant)** and then, click on **Register**.

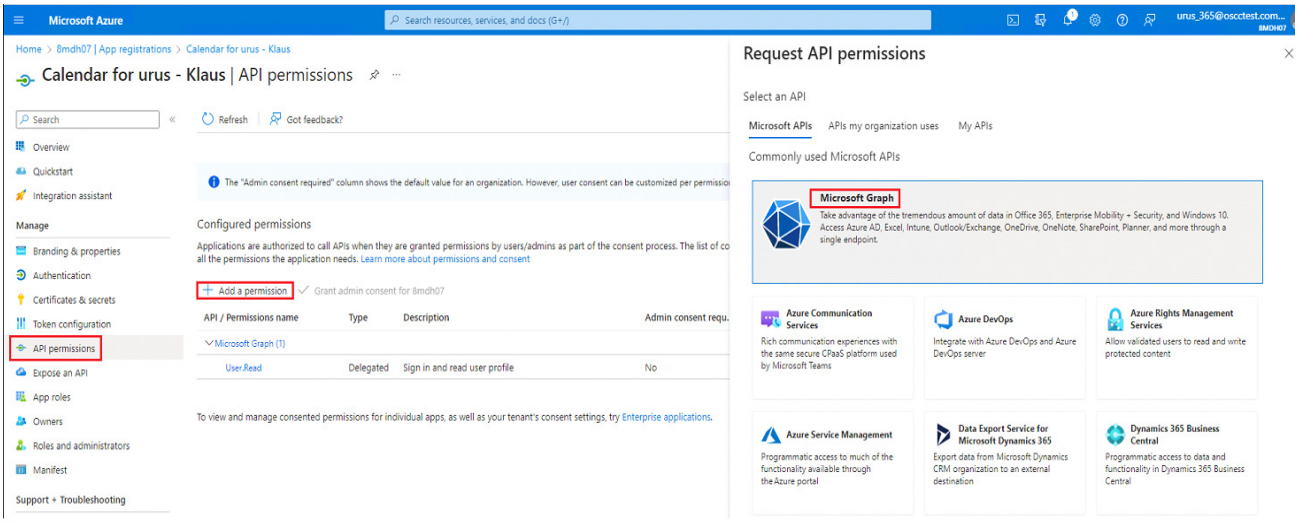


6. Copy and Save the **Application (client) ID and Directory (tenant) ID**.

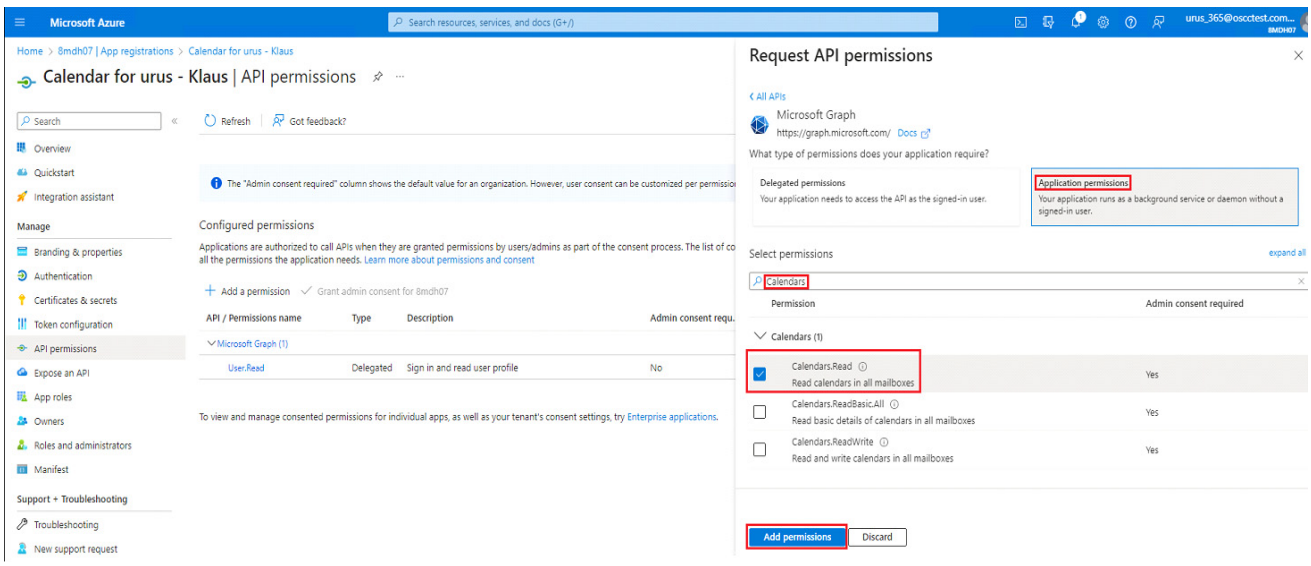
   This information can be copied later from the option **Overview**.



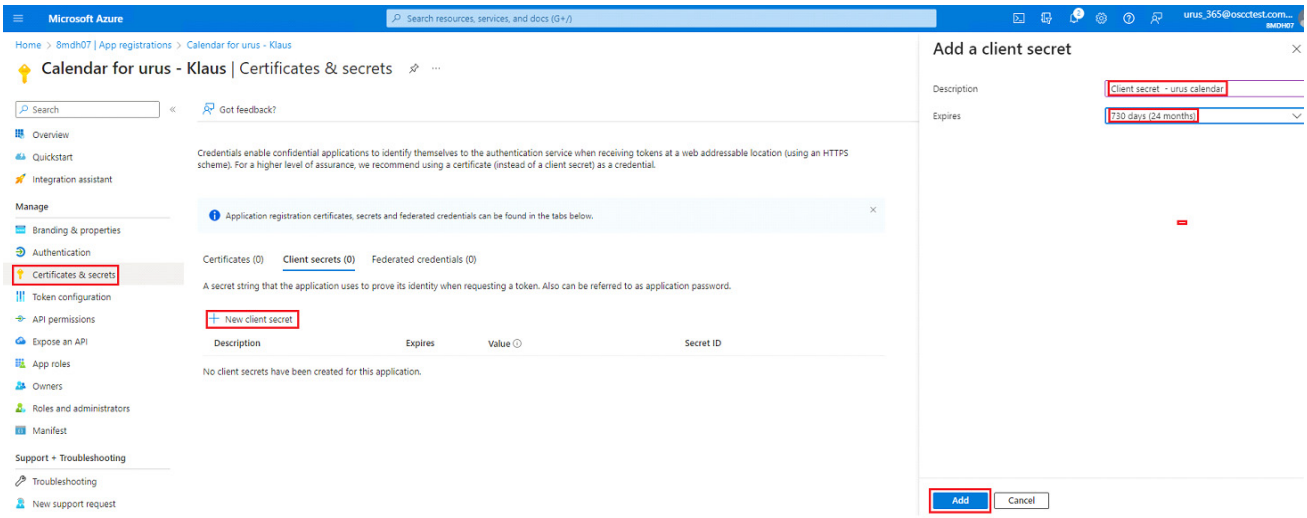
7. Click on **API permissions**, then on Add a permission and on **Microsoft Graph**:



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

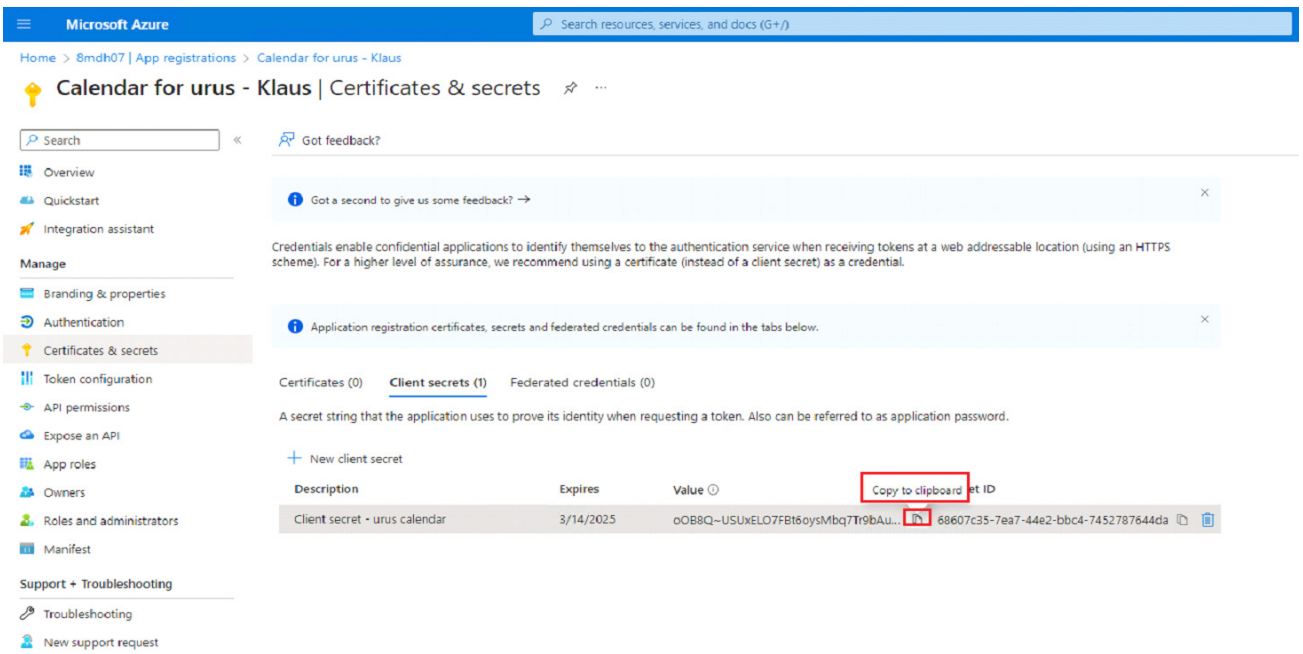


9. Click on **Certificates & secrets**, **New client secret**, enter a **Description**, select when it **Expires** and click on **Add**.



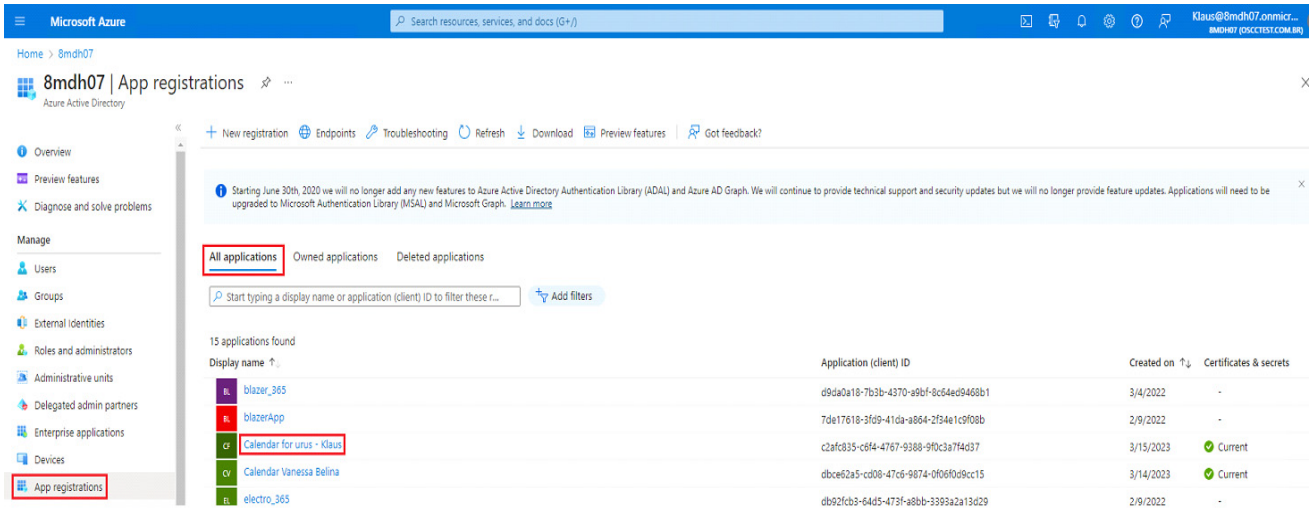
10. Copy this client secret Value and save it.

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.***

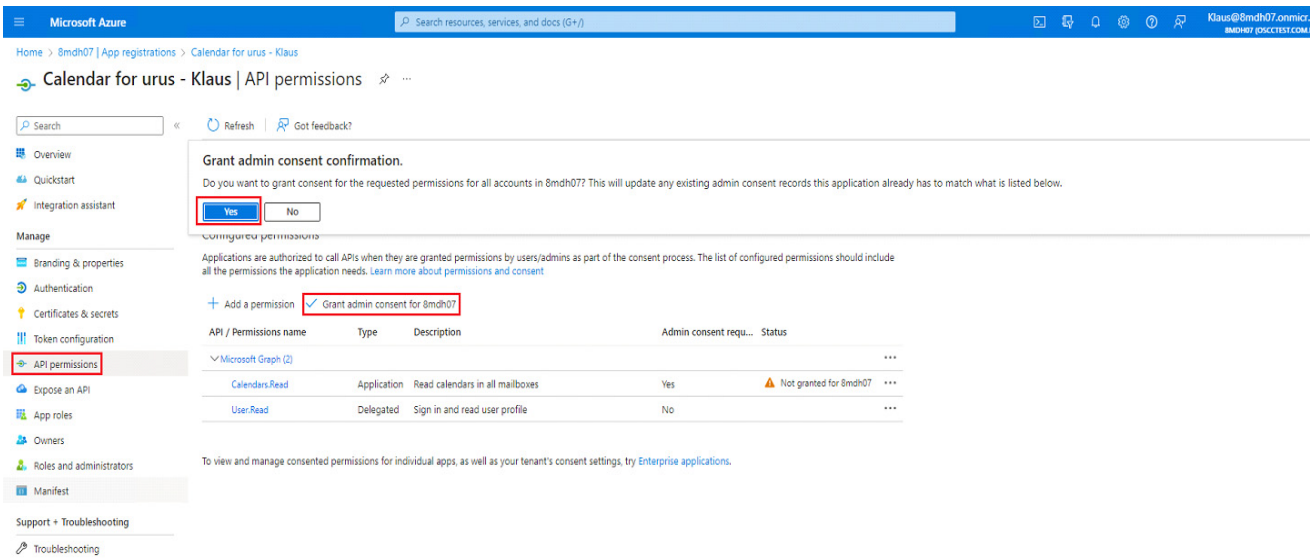


11. Sign out Azure portal, login with administration account.

    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

Apache Tomcat version 19
authentication, e-mail server 17

B

backups, see database backups

C

config.properties
  configuring on a Sun Java System Web Server 26
  configuring on a Tomcat server 24
corporate e-mail server
  configuring 9
  requirements 9
  setting up a secure connection 16
  using authentication 17
corporate Web server
  Apache Tomcat version 19
  configuring 19, 20
  customized files and upgrading 19
  requirements 19
  setting up a secure connection 28
  Sun Java System version 19
  supported operating systems 19
custom e-mail message headers
  about 10
  inserting 13

D

database backups
  full backups 38
  incremental backups 38
  restoring using onbar utility 45
  restoring using ontape utility 42
  scheduling 39
  to a local drive (onbar) 44
  to a local or network drive (ontape) 41
  to a local tape drive (ontape) 40
documentation
  formatting conventions 5, 49
  intended audience 5
  providing feedback 6

E

e-mail message headers
  custom required 10
  inserting custom 13
e-mail reports feature, support for 17
e-mail server 9
  setting up a secure connection 16
  using authentication 17
error codes, for Web callback 30

H

HPWC.ini file
  configuring 22
  enabling for SSL 29

I

IBM Lotus Domino deployment 14
IIS server
  configuring the HPWC.ini file 22
  configuring Web components 21
  creating a virtual directory 22
  setting up a secure connection 29
  testing Web callback 23
IMAP4 protocol 9
Informix
  changing the password 36
  configuring the ontape parameters 39, 41
  using the onbar utility 44
  using the ontape utility 40
IP connections, configuring for wallboards 7
ISAPI extensions 22

L

LDAP directory, configuring for presence integration 34
Lotus Domino deployment 14

M

Microsoft Exchange deployment 12
MIME functions 9

O

OpenScape Contact Center password, changing 36
OpenScape UC Application user account, configuring for presence integration 33

P

passwords, changing 36
presence integration, configuring 33

R

remote service access 35

S

scheduled backups 39
secure connection
  for a corporate e-mail server 16
  for a corporate Web server 28
server machine, shutting down for maintenance 35
SMTP protocol 9
SNMP support, methods 45
SSDP Service Plug-in 35
SSL
  enabling for a corporate e-mail server 16
  enabling for a corporate Web server 28
  enabling on a Sun Java server 29
  enabling on a Tomcat server 29
  enabling on an IIS server 29
Sun Java System Web Server
  configuring and deploying the .war file 26
  configuring Web components 25
  editing config.properties 26
  setting up a secure connection 29
  testing Web callback 27
Sun Java System Web Server version 19

T

Tomcat server
  configuring and deploying the .war file 24
  configuring Web components 23
  editing config.properties 24
  setting up a secure connection 29
  testing Web callback 25

U

utilities
  osccmseheaders 13
utilties
  osccregistersnmpextension 46

V

virtual directory, IIS server 22

W

wallboards, configuring 7
.war file
  configuring on Tomcat server 24
  configuring on a Sun Java System Web Server 26
Web browser requirements 19
Web callback
  error codes 30
  testing on a Tomcat server 25
  testing on an IIS server 23
  testing on Sun Java server 27
Web components
  configuring 20
  configuring on a Sun Java server 25
  configuring on a Tomcat server 23
  configuring on an IIS server 21
  setting up a secure connection 28
  system requirements 19
  Web browser requirements 19
Web server
  Apache Tomcat version 19
  configuring 19, 20
  customized files and upgrading 19
  requirements 19
  setting up a secure connection 28
  Sun Java System version 19
  supported operating systems 19