



A MITEL
PRODUCT
GUIDE

Mitel OpenScape Contact Center Enterprise/ Agile V12

Policy Statements V12

Policy Statements

Planning Guide

10/2024

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>.

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Contents

1 About this document	5
2 Using third-party software to install and patch client applications	7
3 Using third-party software for database backups and system management	9
3.1 Installing database backup software on a server machine	9
3.2 Installing system management software on a server machine	12
3.3 Installing third-party software on a client machine	13
4 Using OpenScape Contact Center software in a virtualized environment	15
4.1 Running server software in a vSphere virtualized environment	15
4.1.1 Main, auxiliary, or central reporting server machine	16
4.1.2 Call Director SIP Service server machine	17
4.1.3 OpenScape Contact Media Service server machine	17
4.2 Running client software in a virtualized environment	18
5 Using a Windows workgroup rather than a domain	21
6 Using Windows service packs and hotfixes with client applications	25
7 Using Microsoft Exchange and IBM Lotus Domino with service packs and hotfixes	27
8 Using untested corporate e-mail servers	31
8.1 Using untested IMAP4 corporate e-mail servers	31
8.2 Using untested SMTP corporate e-mail servers	33
9 Using untested corporate Web servers	35
10 Using untested SAP products	37
10.1 Using the SAP Customer Interaction Center (SAP CIC)	37
10.2 Using the SAP Integrated Communication Interface (SAP ICI)	37
11 Using untested VoiceXML IVR systems	39

1 About this document

This document describes the various policies that apply to the OpenScape Contact Center product and provides recommendations that enable Unify to continue providing support and service to customers who want to use the OpenScape Contact Center product.

The policies described in this document are specific to the OpenScape Contact Center product. General security policies that apply to Unify products, including OpenScape Contact Center, are as follows:

- Support of Operating System Updates for Server Applications Security Policy
http://wiki.unify.com/images/c/c0/Security_Policy_-_Support_of_Operating_System_Updates_for_Server_Applications.pdf
- Support of Virus Protection Software for Server Applications Security Policy
http://wiki.unify.com/images/2/21/Security_Policy_-_Support_of_Virus_Protection_Software_for_Server_Applications.pdf

2 Using third-party software to install and patch client applications

This policy is intended for customers who want to use third-party software to install and patch the OpenScape Contact Center client applications.

This policy describes an approach that addresses this requirement while enabling Unify to continue providing support and service for the OpenScape Contact Center product.

Throughout this document, the term “OpenScape Contact Center client applications” is used to refer to the OpenScape Contact Center Client Desktop, Manager and System Monitor applications.

IMPORTANT: Installing or patching the OpenScape Contact Center client applications incorrectly can adversely affect the operation of the OpenScape Contact Center system and result in Unify being unable to fulfill its support obligation for the OpenScape Contact Center product.

OpenScape Contact Center client applications are packaged using a standard Microsoft Windows Installer (MSI) file. Unify has tested the installation of the client applications by installing the software from the OpenScape Contact Center DVD or from the shared NetSetup folder on the OpenScape Contact Center server machine.

OpenScape Contact Center client software patches are packaged using a standard Microsoft Windows Installer (MSP) file. General patches are deployed by the AutoPA mechanism into the NetSetup\Patch folder on the OpenScape Contact Center server machine. Unify has tested the deployment of patches to the client applications by installing the patches from the shared NetSetup\Patch folder on the OpenScape Contact Center server machine and by installing the patches manually.

Unify understands that customers might want to use third-party software to automate the installation and patching of the OpenScape Contact Center client applications. Doing so will not void the warranty or maintenance agreement with Unify provided that the following occurs.

- The OpenScape Contact Center client installation program is executed to perform the installation.
- All the activities performed by the OpenScape Contact Center installation or patch deployment mechanism are executed.
- The OpenScape Contact Center client applications are correctly installed.

Using third-party software to install and patch client applications

The installation and configuration of third-party software is the sole responsibility of the customer and is accomplished by the customer or their representative at the customer's own risk. The customer assumes all liability should the third-party software interfere with the operation of the OpenScape Contact Center system.

Unify can request that the customer stop using third-party software to install and patch the OpenScape Contact Center client applications if an issue with the operation of the client applications occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories.

If it is determined that the issue was caused by the OpenScape Contact Center client applications being incorrectly installed or patched, Unify can request that the client applications be installed or patched using the standard mechanisms before additional investigations are conducted.

NOTE: For information on how to install and patch the OpenScape Contact Center client applications, see the *OpenScape Contact Center Installation Guide* and the *OpenScape Contact Center Automatic Client Application Installation and Patch Distribution White Paper*.

3 Using third-party software for database backups and system management

This policy is intended for customers who want to install third-party software on an OpenScape Contact Center server machine to perform database backups and system management operations.

This policy describes an approach that addresses this requirement while enabling Unify to continue providing support and service for the OpenScape Contact Center product.

IMPORTANT: Installing third-party software on an OpenScape Contact Center server machine, other than that provided with the OpenScape Contact Center product or described in the OpenScape Contact Center product documentation, can adversely affect the operation and performance of the OpenScape Contact Center system and could result in Unify being unable to fulfill its support obligation for the OpenScape Contact Center product.

3.1 Installing database backup software on a server machine

Unify has tested and recommends using the Informix ontape utility or Informix onbar utility to back up the OpenScape Contact Center database to a local tape drive or a local or network drive.

The Informix onbar utility can also 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: Both utilities are provided with the OpenScape Contact Center system. For information on how to back up and restore the OpenScape Contact Center database using the Informix ontape utility or Informix onbar utility, see the *OpenScape Contact Center System Management Guide*.

Third-party software vendors provide solutions that integrate with Informix and allow backup files to be directed to devices other than tape drives. Unify does not provide, recommend, or certify any other database backup software for use with the OpenScape Contact Center system.

Using third-party software for database backups and system management

Installing database backup software on a server machine

Unify understands that customers might want to install and use third-party software on an OpenScape Contact Center server machine to perform database backups. Doing so will not void the warranty or maintenance agreement with Unify provided that customers adhere to the following guidelines.

- If the installation or operation of the software causes the OpenScape Contact Center system to malfunction, then the customer must do the following:
 1. Uninstall or disable the software to restore proper system operation. The customer can choose to leave the software installed if, in their opinion, the risk of operating without it is greater than the cost of the malfunction.
 2. Report the issue to Unify using the normal product support process.
 3. Reinstall or enable the software after investigation and advice from Unify.
- The creation of backup copies of the OpenScape Contact Center database can be highly CPU and I/O intensive. If database backups are run during high system usage, the backup process will slow system performance and will affect the operation of the OpenScape Contact Center system. This includes the routing of contacts, the collection of statistics, and the delivery of data and events to the OpenScape Contact Center client applications. We recommend that backup copies of the OpenScape Contact Center database be created during periods when the contact center traffic is low. The backup process should also be scheduled such that it does not coincide with the OpenScape Contact Center data maintenance time.
- If required, it is the customer's responsibility to restore the database and verify the recovery of the data. Restoring the database using utilities other than the Informix ontape utility or Informix onbar utility is not covered by Unify service and maintenance contracts and will be a fee-based service if requested by the customer.

The installation and configuration of third-party software is the sole responsibility of the customer and is accomplished by the customer or their representative at the customer's own risk. The customer assumes all liability should the third-party software interfere with the operation of the OpenScape Contact Center system.

Unify can request that the customer stop using the third-party software if an issue with the operation of the system occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories.

Using third-party software for database backups and system management

Installing database backup software on a server machine

If it is determined that the issue was caused by the third-party software, Unify can request that the software be uninstalled before additional investigations are conducted.

Using third-party software for database backups and system management

Installing system management software on a server machine

3.2 Installing system management software on a server machine

Unify does not provide, recommend, or certify specific third-party system management software for use with the OpenScape Contact Center system.

Unify understands that customers might want to install and use third-party system software on an OpenScape Contact Center server machine to accommodate their system management policies. Doing so will not void the warranty or maintenance agreement with Unify provided that customers adhere to the following guidelines.

If the installation or operation of the software causes the OpenScape Contact Center system to malfunction, then the customer must do the following:

1. Uninstall or disable the software to restore proper system operation. The customer can choose to leave the software installed if, in their opinion, the risk of operating without it is greater than the cost of the malfunction.
2. Report the issue to Unify using the normal product support process.
3. Reinstall or enable the software after investigation and advice from Unify.

The installation and configuration of third-party software is the sole responsibility of the customer and is accomplished by the customer or their representative at the customer's own risk. The customer assumes all liability should the third-party software interfere with the operation of the OpenScape Contact Center system.

Unify can request that the customer stop using the third-party software if an issue with the operation of the system occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories.

If it is determined that the issue was caused by the third-party software, Unify can request that the software be uninstalled before additional investigations are conducted.

3.3 Installing third-party software on a client machine

OpenScape Contact Center client applications are installed on client machines containing other business and customer applications. It is the sole responsibility of the customer to ensure proper operation of the client machine.

Unify understands that customers might want to install and use third-party software on an OpenScape Contact Center client machine. Doing so will not void the warranty or maintenance agreement with Unify.

Unify does not place any restrictions on the installation of applications on the client machine. Customers experiencing a malfunction of the OpenScape Contact Center client applications after the installation of software products should report the issue to Unify using the normal product support process.

Unify will endeavor to correct any defects in the OpenScape Contact Center product as per the customer's service agreement with Unify. Malfunctions deemed to be caused by other applications will require correction by the vendor of the application.

Using third-party software for database backups and system management

Installing third-party software on a client machine

4 Using OpenScape Contact Center software in a virtualized environment

This policy is intended for customers who want to run the OpenScape Contact Center software in a VMware vSphere™ virtualized environment.

This policy describes an approach that addresses this requirement while enabling Unify to continue to provide support and service for the OpenScape Contact Center product.

IMPORTANT: Running virtualization software on a physical OpenScape Contact Center server machine is not supported.

4.1 Running server software in a vSphere virtualized environment

The following VMware features have been tested when running the OpenScape Contact Center software on a server machine in a virtualized environment.

- **vSphere vMotion™** – Allows a running virtual machine to be migrated from one physical machine to another without incurring any downtime. This policy covers the vMotion feature being used with vSphere 4.0 (Update 2), 5.0, 5.1, 5.5, 6.0 and 6.5.
- **vSphere High Availability** (V8 R2 and beyond) – Provides protection for OpenScape Contact Center server machines running in a virtualized environment in the event of an operating system or hardware failure. This policy covers the HA feature being used with vSphere 5.0, 5.1, 5.5, 6.0 and 6.5
- **vCenter Site Recovery Manager™** (V8 R1 and beyond) – Helps with the planning, testing, and execution of emergency failovers and the scheduled migration of data center services from one site to another. This policy covers vCenter Site Recovery Manager 5 being used with vSphere 5.0 or 5.1.

Unify understands that customers might want to run the OpenScape Contact Center server software in a vSphere virtualized environment. Doing so will not void the warranty or maintenance agreement with Unify provided that customers adhere to the guidelines described in the following subsections.

NOTE: Since the OpenScape Contact Center software is a real-time application, ensure that sufficient CPU and memory resources are reserved for the virtual machine. For more information, see the *OpenScape Contact Center Running Server Deployments in a VMware vSphere Virtualized Environment White Paper*.

4.1.1 Main, auxiliary, or central reporting server machine

The following OpenScape Contact Center software deployments are covered within the scope of this policy.

- Main server machine
- Auxiliary server machine
- Central reporting server machine

The OpenScape Contact Center server software can be installed on a virtual machine that is running one of the following Microsoft Windows operating systems.

- Windows Server 2016 Datacenter or Enterprise Edition (V9R3 and beyond)
- Windows Server 2012 R2 Standard or Enterprise Edition (V9R0 and beyond)
- Windows Server 2012 R2 Standard or Enterprise Edition with Service Pack 1 (V9R0 and beyond)

If there is an issue with the operation of the OpenScape Contact Center server software in a vSphere virtualized environment, Unify will attempt to reproduce the issue in a non-virtualized environment.

Unify will correct the issue if it can be reproduced in such an environment. Unify can request that the customer report the issue to the VMware product support team if a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories.

If it is determined that the issue was caused by the programming techniques or tools used by Unify, Unify will consider modifying the OpenScape Contact Center server software if the modification is found to be consistent with operating the software in a non-virtualized environment.

4.1.2 Call Director SIP Service server machine

The Call Director SIP Service software can be installed on a virtual machine (V8R1, V8R2, V9R0 and V9R1).

If there is an issue with the operation of the OpenScape Contact Center server software in a vSphere virtualized environment, Unify will attempt to reproduce the issue in a non-virtualized environment.

Unify will correct the issue if it can be reproduced in such an environment. Unify can request that the customer report the issue to the VMware product support team if a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories.

If it is determined that the issue was caused by the programming techniques or tools used by Unify, Unify will consider modifying the OpenScape Contact Center server software if the modification is found to be consistent with operating the software in a non-virtualized environment.

4.1.3 OpenScape Contact Media Service server machine

The OpenScape Contact Media Service software can be installed on a virtual machine (V9R2 and beyond).

If there is an issue with the operation of the OpenScape Contact Media Service server software in a vSphere virtualized environment, Unify will attempt to reproduce the issue in a non-virtualized environment.

Unify will correct the issue if it can be reproduced in such an environment. Unify can request that the customer report the issue to the VMware product support team if a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories.

If it is determined that the issue was caused by the programming techniques or tools used by Unify, Unify will consider modifying the OpenScape Contact Media Service server software if the modification is found to be consistent with operating the software in a non-virtualized environment.

4.2 Running client software in a virtualized environment

Unify understands that customers might want to run the OpenScape Contact Center client software in a virtualized environment using products such as Citrix Presentation Server, Windows Terminal Services, or VMware. Doing so will not void the warranty or maintenance agreement with Unify.

The OpenScape Contact Center client software has been designed using Microsoft-approved programming techniques and tools. The following OpenScape Contact Center software deployments are known to operate normally in a virtualized environment and are covered within the scope of this policy.

- Client Desktop (Agent, Associate, Attendant Console)
- Manager
- Screen Pop API

NOTE: Other OpenScape Contact Center client applications are not to be used in a virtualized environment unless the applications are running on a virtualized server machine, in which case the policy in [Section 4.1.1, “Main, auxiliary, or central reporting server machine”](#) applies.

The Agent Portal Java (V9R0 and beyond) was not tested with any virtualized environment. However, since the Agent Portal is a Java Web Start application it is expected to work.

The Agent Portal Web (V9R3 and beyond) has not been tested with any virtualized environment. However, since the Agent Portal Web is a pure web application it is expected to work. The OpenScape Contact Center client software can be installed on a virtual machine that is running one of the following Microsoft Windows operating systems.

- Windows Server 2016 Datacenter or Enterprise Edition (V9R3 and beyond)
- Windows Server 2012 R2 Standard or Enterprise Edition (V9R0 and beyond)
- Windows Server 2012 R2 Standard or Enterprise Edition with Service Pack 1 (V9R0 and beyond)
- Windows 10 Professional or Enterprise Edition
- Windows 8 or 8.1 Professional or Enterprise Edition
- Windows 7 Professional or Enterprise Edition

Using OpenScape Contact Center software in a virtualized environment

Running client software in a virtualized environment

If there is an issue with the operation of an OpenScape Contact Center client application in a virtualized environment, Unify will attempt to reproduce the issue using a Windows client machine in a non-virtualized environment.

Unify will correct the issue if it can be reproduced in such an environment. Unify can request that the customer report the issue to the appropriate virtualization vendor's product support team if a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories.

If it is determined that the issue was caused by the programming techniques or tools used by Unify, Unify will consider modifying the OpenScape Contact Center client applications if the modification is found to be consistent with operating the software using a Windows client machine in a non-virtualized environment.

Using OpenScape Contact Center software in a virtualized environment

Running client software in a virtualized environment

5 Using a Windows workgroup rather than a domain

This policy is intended for customers who want to run the OpenScape Contact Center system on a machine that is configured to be a member of a Windows workgroup rather than a domain.

This policy describes an approach that addresses this requirement while enabling Unify to continue to provide support and service for the OpenScape Contact Center product.

IMPORTANT: Running the OpenScape Contact Center system on a machine that is configured as a member of a Windows workgroup rather than a domain can adversely affect the operation of the OpenScape Contact Center system and could result in Unify being unable to fulfill its support obligation for the OpenScape Contact Center product.

Unify has tested the OpenScape Contact Center system with various machines configured as members of a domain rather than a workgroup.

Unify understands that customers might want to run the OpenScape Contact Center system on a machine that has been configured as a member of a workgroup rather than a domain. Doing so will not void the warranty or maintenance agreement with Unify provided that customers adhere to the following guidelines.

- The Windows account under which the HiPath ProCenter service operates (by default “hppc”) must be the same on the main server machine and any auxiliary server machines. In other words, the same user ID and password must be used on each of the machines and the account must have sufficient rights to access the appropriate network shares on the main server machine.

Alternatively, each auxiliary server machine can be configured with a user ID that has sufficient rights to access the appropriate network shares on the main server machine.

NOTE: For OpenScape Contact Center, a network share must explicitly be established from a client machine that is running the Manager application to the main server machine, using a user ID that has sufficient rights on the main server machine to access the appropriate network shares that are used by the Manager application.

Using a Windows workgroup rather than a domain

- The AutoPA feature will function correctly with OpenScape Contact Center server machines that belong to a workgroup rather than a domain. However, the Windows account under which the HiPath ProCenter AutoPA service operates must be the same on the main server machine and any auxiliary server machines. In other words, the same user ID and password must be used on each of the machines.
- All OpenScape Contact Center server machines must have their computer clocks synchronized with one another through the use of a common Time Server. This applies for configurations where the main server machine is operating in conjunction with auxiliary server machines and in multisite environments where the OpenScape Contact Center networking or central reporting features are in use.

NOTE: In a multisite environment, the OpenScape Contact Center server machines must have their computer clocks synchronized, but do not have to be in the same time zone.

- If the OpenScape Contact Center client machines are configured to be members of a domain and the OpenScape Contact Center server machines are members of a workgroup, then the Windows authentication mechanism can still be configured for users to access the OpenScape Contact Center system. However, if the client machines are also members of a workgroup, it is recommended that the OpenScape Contact Center authentication mechanism be used instead.
- For OpenScape Contact Center, if the Manager application is being run on a machine other than the main server machine, one of the following must occur.
 - The Windows account under which the Manager application is being run must exist on both the main server machine and the client machine on which the application is being run. In other words, the same user ID and password must be configured on both machines and the account must have sufficient rights to access the appropriate network shares on the main server machine.
 - Each client machine must be configured with a user ID that has sufficient rights to access the appropriate network shares on the main server machine that are used by the Manager application.

- If the central reporting feature is in use, the Windows account under which the Informix service operates (by default, "informix") must be the same on each main server machine and the central reporting server machine. In other words, the same user ID and the same password must be used on each of the machines.
- The high availability (warm standby) feature requires that domain accounts be used to support Windows clustering, and therefore this feature is not supported when the server machines are members of a workgroup only.

The configuration of a machine as a member of a workgroup is the sole responsibility of the customer or their representative and is accomplished at the customer's own risk. The customer assumes all liability should the configuration interfere with the operation of the OpenScape Contact Center system.

Unify can request that the customer stop using the OpenScape Contact Center system in a workgroup configuration if an issue with the operation of the system occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories using a Windows configuration where all of the machines are members of a domain.

If it is determined that the issue was caused by the customer's workgroup configuration, Unify can request that the Windows configuration be changed such that all of the machines are operating as members of a domain before additional investigations are conducted.

Customers can choose to report issues to Microsoft, indicating that a failure was not observed when the same software was operating in a domain configuration.

Using a Windows workgroup rather than a domain

6 Using Windows service packs and hotfixes with client applications

This policy is intended for customers who want to install Windows service packs and hotfixes that have not been tested by Unify on an OpenScape Contact Center client machine.

This policy describes an approach that addresses this requirement while enabling Unify to continue to provide support and service for the OpenScape Contact Center product.

Windows Service packs are a collection of corrections, improvements and new functionality for the Windows platform that typically cover all aspects of the Windows operating system. Hotfixes are individual corrections or improvements to the Windows platform that typically address urgent security or reliability concerns.

Unify understands that customers might want to install Windows service packs or hotfixes on a client machine that is running OpenScape Contact Center client applications and other business and customer applications. Doing so will not void the warranty or maintenance agreement with Unify.

Unify does not place any restrictions on the installation of Windows service packs or hotfixes on a client machine. It is the sole responsibility of the customer to ensure the proper installation and verification of Windows service packs and hotfixes.

If the application of the Windows service pack or hotfix causes the system to malfunction, then the customer should report the issue to Unify using the normal product support process.

7 Using Microsoft Exchange and IBM Lotus Domino with service packs and hotfixes

This policy is intended for customers who are using Microsoft Exchange or IBM Lotus Domino as their corporate e-mail server and want to install service packs and hotfixes on the corporate e-mail server.

This policy describes an approach that addresses this requirement while enabling Unify to continue to provide support and service for the OpenScape Contact Center product.

Service packs are a collection of corrections, improvements and new functionality for the Microsoft Exchange or IBM Lotus Domino platform that typically cover all aspects of the system. Hotfixes are individual corrections or improvements to the Microsoft Exchange or IBM Lotus Domino platform that typically address urgent security or reliability concerns.

Unify has tested the following corporate e-mail servers in conjunction with the OpenScape Contact Center system.

- Microsoft Office 365
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- IBM Lotus Domino 9
- Google Gmail

Prior to releasing a new or updated version of the OpenScape Contact Center product, Unify will test the integration with the Microsoft Exchange and IBM Lotus Domino platforms based on the following guidelines.

- Unify will test the latest generally available version and service pack for Microsoft Exchange and IBM Lotus Domino.
- Unify will concurrently test a selection of hotfixes for the release or service pack.
- Customers upgrading their OpenScape Contact Center systems will be asked to apply the tested Microsoft Exchange or IBM Lotus Domino service pack and hotfixes to their systems.

Using Microsoft Exchange and IBM Lotus Domino with service packs and hotfixes

Unify understands that customers might want to install Microsoft Exchange or IBM Lotus Domino service packs or hotfixes prior to the completion of testing by Unify. Doing so will not void the warranty or maintenance agreement with Unify provided that customers adhere to the following guidelines.

If the application of the Microsoft Exchange or IBM Lotus Domino service pack or hotfix causes the system to malfunction, then the customer should:

1. Report the issue to the appropriate vendor's product support team indicating that an upgrade to Microsoft Exchange or IBM Lotus Domino has caused a previously-working application to fail.
2. Report the issue to Unify using the normal support process so that investigation and testing can be initiated in the Unify laboratories in parallel to the Microsoft or IBM activities.
3. Uninstall the Microsoft Exchange or IBM Lotus Domino service pack or hotfix to restore proper system operation. The customer can choose to leave the service pack or hotfix installed if, in their opinion, the risk of operating without it is greater than the cost of the malfunction.
4. Reapply the Microsoft Exchange or IBM Lotus Domino service pack or hotfix after investigation and advice from Microsoft, IBM, or Unify.

The installation of service packs and hotfixes from Microsoft or IBM is the sole responsibility of the customer and is accomplished by the customer or their representative at the customer's own risk. The customer assumes all liability should the installed service pack or hotfix interfere with the operation of the OpenScape Contact Center system.

Unify can request that the customer stop using the OpenScape Contact Center e-mail feature and e-mailing reports if an issue with the operation of the system occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories.

If it is determined that the issue was caused by an installed service pack or hotfix, Unify can request that the service pack or hotfix be uninstalled before additional investigations are conducted.

Customers can choose to report the issue to Microsoft or IBM indicating that a failure was not observed with the versions of Microsoft Exchange or IBM Lotus Domino that have been tested by Unify.

8 Using untested corporate e-mail servers

This policy is intended for customers who want to use a corporate e-mail server that has not been tested by Unify to support the OpenScape Contact Center e-mail feature and the e-mailing of reports.

This policy describes an approach that addresses this requirement while enabling Unify to continue to provide support and service for the OpenScape Contact Center product.

Unify does not provide a corporate e-mail server for use with the OpenScape Contact Center system. Unify has tested the following corporate e-mail servers in conjunction with the OpenScape Contact Center system.

- Microsoft Office 365
- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- IBM Lotus Domino 9
- Google Gmail

IMPORTANT: Using a corporate e-mail server that has not been tested by Unify can adversely affect the operation of the OpenScape Contact Center e-mail feature and the e-mailing of reports and could result in Unify being unable to fulfill its support obligation for the OpenScape Contact Center product.

8.1 Using untested IMAP4 corporate e-mail servers

Unify understands that customers might want to use an IMAP4 corporate e-mail server other than Microsoft Exchange or IBM Lotus Domino or a version of Microsoft Exchange or IBM Lotus Domino that has not been tested by Unify. Doing so will not void the warranty or maintenance agreement with Unify provided that customers adhere to the following guidelines.

- The IMAP4 corporate e-mail server must comply with RFC-2060 for interfacing with IMAP4 clients. In particular, the IMAP4 corporate e-mail server must provide the following functionality required by the OpenScape Contact Center system to support the OpenScape Contact Center e-mail feature and the e-mailing of reports.

Using untested corporate e-mail servers

Using untested IMAP4 corporate e-mail servers

- The ability to have a dedicated OpenScape Contact Center user account.
- The ability to reserve a specific Inbox as the primary incoming mailbox for the dedicated OpenScape Contact Center user account.
- The ability to have multiple concurrent IMAP sessions connecting to the dedicated OpenScape Contact Center user account when the e-mail reports feature is used in conjunction with the high availability (warm standby) or central reporting feature.
- The ability to create up to 30,000 messages per e-mail folder. This is the maximum daily capacity to support the OpenScape Contact Center e-mail feature and the e-mailing of reports.
- The ability to create and delete e-mail folders.
- The ability to support the following IMAP4 functions.
 - APPEND
 - CHECK
 - COPY
 - CREATE
 - DELETE
 - EXPUNGE
 - FETCH
 - LIST
 - LOGIN
 - LOGOUT
 - NOOP
 - SEARCH
 - SELECT
 - STATUS
 - STORE
 - UID FETCH

- UID SEARCH

NOTE: The OpenScape Contact Center system also supports the use of SSL/TLS for IMAP4 communications, as a configurable option, by tunneling IMAP4 over SSL/TLS.

The installation and configuration of an untested IMAP4 corporate e-mail server is the sole responsibility of the customer and is accomplished by the customer or their representative at the customer's own risk. The customer assumes all liability should the untested IMAP4 corporate e-mail server interfere with the operation of the OpenScape Contact Center system.

Unify can request that the customer stop using the OpenScape Contact Center e-mail functionality if an issue with the operation of the system occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories using Microsoft Exchange or IBM Lotus Domino.

If it is determined that the issue was caused by the untested IMAP4 corporate e-mail server, Unify can request that the IMAP4 corporate e-mail server be replaced with either Microsoft Exchange or IBM Lotus Domino before additional investigations are conducted.

Customers can choose to report the issue to the vendor of the untested IMAP4 corporate e-mail server indicating that a failure was not observed with the versions of Microsoft Exchange or IBM Lotus Domino that have been tested by Unify.

8.2 Using untested SMTP corporate e-mail servers

Unify understands that customers might want to use an SMTP corporate e-mail server other than Microsoft Exchange or IBM Lotus Domino or a version of Microsoft Exchange or IBM Lotus Domino that has not been tested by Unify. Doing so will not void the warranty or maintenance agreement with Unify provided that customers adhere to the following guidelines.

- The SMTP corporate e-mail server must comply with RFC-821, RFC-822, RFC-974, RFC-1854, RFC-1869, RFC-1891, RFC-2045, RFC-2046 and RFC-2047 for creating and sending e-mail messages. In particular, the SMTP corporate e-mail server must provide the following functionality required by the OpenScape Contact Center system to support e-mail functionality.

Using untested corporate e-mail servers

Using untested SMTP corporate e-mail servers

- The ability to send e-mail messages with From addresses that are different than the From address that is associated with the dedicated OpenScape Contact Center user account when e-mailing reports.
- The ability to support the following SMTP functions.
 - SEND
 - NOOP
 - MAIL FROM
- To support the use of SSL/TLS (using the STARTTLS mechanism) for SMTP communications, which is a configurable option in the Manager application, the SMTP corporate e-mail server must comply with RFC-3207.
- To support user authentication (using the ESMTP AUTH LOGIN mechanism) for SMTP communications, which is configurable option in the Manager application, the SMTP corporate e-mail server must comply with RFC-2554.

The installation and configuration of an untested SMTP corporate e-mail server is the sole responsibility of the customer and is accomplished by the customer or their representative at the customer's own risk. The customer assumes all liability should the untested SMTP corporate e-mail server interfere with the operation of the OpenScape Contact Center system.

Unify can request that the customer stop using the OpenScape Contact Center e-mail functionality if an issue with the operation of the system occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories using Microsoft Exchange or IBM Lotus Domino.

If it is determined that the issue was caused by the untested SMTP corporate e-mail server, Unify can request that the corporate e-mail server be replaced with either Microsoft Exchange or IBM Lotus Domino before additional investigations are conducted.

Customers can choose to report the issue to the vendor of the untested SMTP corporate e-mail server indicating that a failure was not observed with the versions of Microsoft Exchange or IBM Lotus Domino that have been tested by Unify.

9 Using untested corporate Web servers

This policy is intended for customers who want to use a corporate Web server that has not been tested by Unify to support the OpenScape Contact Center Web collaboration, Web callback, or VoiceXML integration features.

This policy describes an approach that addresses this requirement while enabling Unify to continue to provide support and service for the OpenScape Contact Center product.

Unify does not provide a corporate Web server for use with the OpenScape Contact Center system. Unify has tested the following corporate Web server platforms in conjunction with the OpenScape Contact Center system.

- Microsoft Internet Information Server (IIS) 10 on Windows Server 2016 (V9R3 and beyond)
- Microsoft Internet Information Server (IIS) 8.5 on Windows Server 2012 R2 (V9R0 and beyond)
- Microsoft Internet Information Server (IIS) 7.5 on Windows Server 2008 R2 (V8 R1 and R2 only)
- Sun Java System Web Server 6.1 or 7.0 on Sun Solaris 9
- Apache Tomcat 7.0 on Red Hat Enterprise Linux 6 Server
- Apache Tomcat 6.0 on Red Hat Enterprise Linux 6 Server

NOTE: VoiceXML integration has not been tested on a Sun Java System Web Server.

IMPORTANT: Using a corporate Web server that has not been tested by Unify can adversely affect the operation of the OpenScape Contact Center Web functionality and could result in Unify being unable to fulfill its support obligation for the OpenScape Contact Center product.

Unify understands that customers might want to use a corporate Web server platform that has not been tested by Unify. Doing so will not void the warranty or maintenance agreement with Unify provided that customers adhere to the following guidelines.

- IIS-compatible corporate Web server platforms must support standard ISAPI extensions.

Using untested corporate Web servers

- Java-based corporate Web server platforms must support servlet specification 2.4 or later and JDK 1.5.

The installation and configuration of an untested corporate Web server is the sole responsibility of the customer and is accomplished by the customer or their representative at the customer's own risk. The customer assumes all liability should the untested corporate Web server interfere with the operation of the OpenScape Contact Center system.

Unify can request that the customer stop using the OpenScape Contact Center Web functionality if an issue with the operation of the system occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories using a tested corporate Web server platform.

If it is determined that the issue was caused by the untested corporate Web server, Unify can request that the corporate Web server be replaced with a tested corporate Web server platform before additional investigations are conducted.

Customers can choose to report the issue to the vendor of the untested corporate Web server or to the vendor of the operating system on which the corporate Web server is installed indicating that a failure was not observed with the versions of the corporate Web server platforms that have been tested by Unify.

10 Using untested SAP products

This policy is intended for customers who want to use an SAP product that has not been tested by Unify to integrate with the OpenScape Contact Center system.

This policy describes an approach that addresses this requirement while enabling Unify to continue to provide support and service for the OpenScape Contact Center product.

IMPORTANT: Using an SAP product that has not been tested by Unify can adversely affect the operation of the OpenScape Contact Center SAP Integration features and could result in Unify being unable to fulfill its support obligation for the OpenScape Contact Center product.

10.1 Using the SAP Customer Interaction Center (SAP CIC)

Customers can choose to report the issue to SAP indicating that a failure was not observed with the SAP product that has been tested by Unify.

10.2 Using the SAP Integrated Communication Interface (SAP ICI)

Unify has tested the OpenScape Contact Center SAP ICI Desktop Integration with the following:

- OpenScape Contact Center V9 - SAP CRM 4.0 and SAP CRM 5.0 certified with the SAP CA-ICI-CTI 3.00 Interface.
- OpenScape Contact Center V9 R1 - SAP CRM 5.0 and SAP CRM 7.0 certified with the SAP CA-ICI-CTI 3.06 Interface.
- OpenScape Contact Center V9 R2 and beyond - SAP CRM 7.0 certified with the SAP CA-ICI-CTI 3.07 Interface.

Unify understands that customers might want to use a SAP product that has not been tested by Unify. Doing so will not void the warranty or maintenance agreement with Unify when it is compatible with the supported SAP CA-ICI-CTI Interface.

The installation and configuration of an untested SAP product is the sole responsibility of the customer and is accomplished by the customer or their representative at the customer's own risk. It is the

Using untested SAP products

Using the SAP Integrated Communication Interface (SAP ICI)

customer's responsibility to confirm that the SAP product that they want to use is compatible with the supported SAP CA-ICI-CTI Interface. The customer assumes all liability should the untested SAP product interfere with the operation of the OpenScape Contact Center system.

Unify can request that the customer stop using the SAP product if an issue with the operation of the system occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories.

Customers can choose to report the issue to SAP indicating that a failure was not observed with the SAP product that has been tested by Unify.

11 Using untested VoiceXML IVR systems

This policy is intended for customers who want to use the OpenScape Contact Center VoiceXML Integration feature with a VoiceXML IVR system that has not been tested by Unify.

This policy describes an approach that addresses this requirement while enabling Unify to continue to provide support and service for the OpenScape Contact Center product.

Unify has tested the following VoiceXML IVR systems in conjunction with the OpenScape Contact Center system.

- Genesys Voice Platform V7.6
- OpenScape Contact Center Voice Portal V7.0 R3

IMPORTANT: Using a VoiceXML IVR system that has not been tested by Unify can adversely affect the operation of the OpenScape Contact Center VoiceXML Integration feature and could result in Unify being unable to fulfill its support obligation for the OpenScape Contact Center product.

Unify understands that customers might want to use the OpenScape Contact Center VoiceXML Integration with a VoiceXML IVR system that has not been tested by Unify. Doing so will not void the warranty or maintenance agreement with Unify provided that customers adhere to the following guidelines.

- The VoiceXML IVR system must comply with the VoiceXML 2.0 standard. The OpenScape Contact Center VoiceXML Integration functionality is provided through a set of VoiceXML subdialogs. The VoiceXML IVR system must support the invocation of VoiceXML subdialogs.
- The VoiceXML IVR system must be able to provide an identifier for a particular VoiceXML session (such as a channel number and host name combination), which uniquely identifies the session among all other sessions that are interacting with the OpenScape Contact Center VoiceXML Integration feature.

The installation and configuration of an untested VoiceXML IVR system is the sole responsibility of the customer and is accomplished by the customer or their representative at the customer's own risk. The customer assumes all liability should the untested VoiceXML IVR system interfere with the operation of the OpenScape Contact Center system.

Using untested VoiceXML IVR systems

Unify can request that the customer stop using the OpenScape Contact Center VoiceXML Integration feature if an issue with the operation of the system occurs and a proper diagnosis of the issue cannot be performed with reasonable effort in the Unify laboratories using a tested VoiceXML IVR system.

If it is determined that the issue was caused by the untested VoiceXML IVR system, Unify can request that the VoiceXML IVR system be replaced with a tested VoiceXML IVR system before additional investigations are conducted.

Customers can choose to report the issue to the vendor of the untested VoiceXML IVR system indicating that a failure was not observed with the VoiceXML IVR systems that have been tested by Unify.

