



Avaya Experience Platform™ Workforce Engagement

Technology, Security, & Network Integration
Deployment Reference Guide

Version 15.2

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by Avaya. You agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by You.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:

<http://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"**Hosted Service**" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE AVAYA GLOBAL SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO](http://support.avaya.com/licenseinfo), OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS THE SOFTWARE (AS DEFINED IN THE AVAYA GLOBAL SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS), AND WHO PURCHASED THE LICENSE FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. REFER TO THE AVAYA SOFTWARE LICENSE TERMS FOR VERINT SOFTWARE PRODUCTS FOR INFORMATION REGARDING THE APPLICABLE LICENSE TYPES PERTAINING TO THE SOFTWARE.

All Rights Reserved

Avaya and/or its licensors retain title to and ownership of the Software, Documentation, and any modifications or copies thereof. Except for the limited license rights expressly granted in the applicable Avaya Global Software License Terms for Verint Software Products, Avaya and/or its licensors reserve all rights, including without limitation copyright, patent, trade secret, and all other intellectual property rights, in and to the Software and Documentation and any modifications or copies thereof. The Software contains trade secrets of Avaya and/or its licensors, including but not limited to the specific design, structure and logic of individual Software programs, their interactions with other portions of the Software, both internal and external, and the programming techniques employed.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

Certain software programs or portions thereof included in the Software may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for any Software that has distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Software, Documentation or on Avaya's website at: <http://support.avaya.com/Copyright> (or a successor site as designated by Avaya). The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com)

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE [WWW.SIPRO.COM/CONTACT.HTML](http://www.sipro.com/contact.html). THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Software is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud Intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <http://support.avaya.com>, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security> Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, any Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website:

<http://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <http://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <http://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

About this guide	4
Introduction to the Avaya Experience Platform™ Workforce Engagement deployment	6
Avaya Experience Platform™ Workforce Engagement overview	7
Avaya Experience Platform™ Workforce Engagement connectivity	9
Networking in cloud deployments	12
Network connectivity	13
Network security	15
Bandwidth, latency, ports, and connection types	16
Bandwidth and latency requirements	17
Port requirements	20
User authentication in cloud deployments	22
User authentication methods	23
User authentication principles	23
User authentication matrix	24
DB Realm customer requirements	25
SAML customer requirements	26
OpenID Connect for mobile customer requirements	27
Archiving in cloud deployments	30
Supported archive devices	31
Fixed media definition fields	32
Client application management	35
Desktop applications	36
Desktop antivirus requirements	36
Mobile applications	38
Applications	38
Mobile device management	38

About this guide

This guide describes the technology, networking, and security requirements for customers when connecting to the SaaS Avaya Experience Platform™ Workforce Engagement.

The guide covers cloud deployment of the Workforce Optimization (WFO) solution, which includes the following major application families:

- Interaction-based products that include Recording, Quality Management (QM), Automated Quality Management (AQM), and Interaction Analytics
- Workforce Management (WFM) and Performance Management (PM)
- Desktop and Processes Analytics (DPA)

Customers deploying some of the WFO products, need to focus only on the sections that are relevant to their deployments.

This guide does not cover hybrid cloud deployments, where WFO recording and transcription servers are deployed on-premises or on a 3rd party cloud under the responsibility of the customer.

Intended Audience

This guide is for customers and prospective customers who need to understand what is required of them to use the products in the SaaS Avaya Experience Platform™ Workforce Engagement.

Document revision history

Revision	Description of changes
1.18	Minor updates.
1.17	Rebranded Avaya OneCloud CCaaS to Avaya Experience Platform™.
1.16	Updated the technology stack as part of 2022R1 updates.

Revision	Description of changes
1.16	<i>Network security</i> : Added a note that customers using Azure AD to integrate with VCP Identity are not required to track SAML certificates.
1.15	In <i>Desktop antivirus requirements</i> , added "Notes on antivirus exclusions for Desktop and Process Analytics (DPA)."
1.14	<i>Network connectivity</i> : Clarified the TLS and VPN connectivity options.
1.13	Minor text corrections
1.12	Minor updates
1.11	In the <i>Communication between desktops and sites (including data center)</i> topic, updated the bandwidth requirements when recorders are on the data center and when the recorders are on the site.
1.10	<ul style="list-style-type: none"> Update terminology for Avaya Experience Platform™ Workforce Engagement
1.09	<ul style="list-style-type: none"> Under 'Bandwidth and Latency' section, change Voice Recording (streaming) bandwidth to 8.08 Mbps.
1.08	<ul style="list-style-type: none"> Updates to indicate that VPN is an alternative to DX based on cost performance considerations.
1.07	Under 'Bandwidth and latency requirements', update the Screen recording values.
1.06	<ul style="list-style-type: none"> Defect fixes
1.05	<ul style="list-style-type: none"> Minor updates
1.04	Updated the latency for voice and video recording (streaming)
1.03	<ul style="list-style-type: none"> Add new table for WFO desktop user activity bandwidth requirements Add NAT guidelines
1.02	2020R1 updates: <ul style="list-style-type: none"> Verint rebranding.
1.01	Added ADFS as a new supported OpenID Connect provider (as of WFO Package 722 or later).
1.00	Initial release

Introduction to the Avaya Experience Platform™ Workforce Engagement deployment

Avaya Experience Platform™ Workforce Engagement deployment is a zero footprint SaaS offering where all Workforce Optimization (WFO) services are provided in the cloud. The Service Provider manages all the cloud-based services.

In cloud deployments, the communication infrastructure (such as telephony switch and ACD), is either on customer site (on-premises) or cloud-based.

Desktop and mobile applications are the responsibility of the customer.

Topics

Avaya Experience Platform™ Workforce Engagement overview	7
Avaya Experience Platform™ Workforce Engagement connectivity	9

Avaya Experience Platform™ Workforce Engagement overview

The Avaya Experience Platform™ Workforce Engagement deployment includes WFO services, communication infrastructure, desktop devices, mobile devices (optional), archive storage (if relevant), and Identify Provider (IdP).

Cloud WFO services

The cloud is composed of the following key WFO services:

- **Databases services:** Store and index the data required for each business application.
- **Application services:** Support the user facing business applications. WFO includes the following major application families:
 - Interaction-based products that include Recording, Quality Management (QM), Automated Quality Management (AQM), and Interaction Analytics
 - Workforce Management (WFM) and Performance Management (PM)
 - Desktop and Processes Analytics (DPA)
- **Integration services:** Integrate directly to the communication infrastructure. Receive CTI data events and WFM/PM data feeds needed to support the recording and the WFM/Performance Management applications, respectively.
- **Recording services:** Receive communication content in the form of media for deployments with recording.
- **Speech transcription services:** Generate the transcription of voice media interactions.

Communication infrastructure

The communication infrastructure, such as switch/ACD, provides CTI data events, communication content, and WFM/PM data feeds to the Avaya Experience Platform™ Workforce Engagement integration and recording services. The communication infrastructure is the responsibility of the customer and is deployed either on the customer site (on-premises) or on a 3rd party cloud.

Desktop and mobile devices

Employees use desktops and mobile devices to interact with the Avaya Experience Platform™ Workforce Engagement services:

- Agent desktops include services for capturing employee-generated data such as screen recordings, DPA events, and Face to Face recordings.
- WFO user desktops include user-facing applications such as WFM, Performance Management, Speech Analytics, and Interactions.
- Mobile applications include user-facing applications accessible from mobile devices, such as WFM applications.

WFO user and agent desktops are deployed either on-premises or in a remote location such home desktops.

Archive storage

For WFO solutions that include recording, archive storage is used to archive the recorded content. Archive storage is either provided by the service provider or by the customer:

- When provided by the service provider, archive storage it is deployed on the Avaya Experience Platform™ Workforce Engagement
- When provided by the customer, archive storage can either be deployed on a 3rd party cloud, or on-premises, if the communication infrastructure is located on-premises.

For example, archive storage can be on Amazon web services, using customer-supplied S3 archive storage.

Identity provider (IdP)

The customer can either use a third-party vendor IdP to manage their WFO identities, or request the service provider to manage them. If an external IdP is used, the WFO user desktop and mobile applications communicate with the IdP. The IdP is the responsibility of the customer, and is located either on a 3rd party cloud, or on-premises.

Related topics

[Avaya Experience Platform™ Workforce Engagement connectivity](#), page 9

Related information

The relevant Cloud Recorder Integration guide

The relevant Cloud WFM Interfaces guide

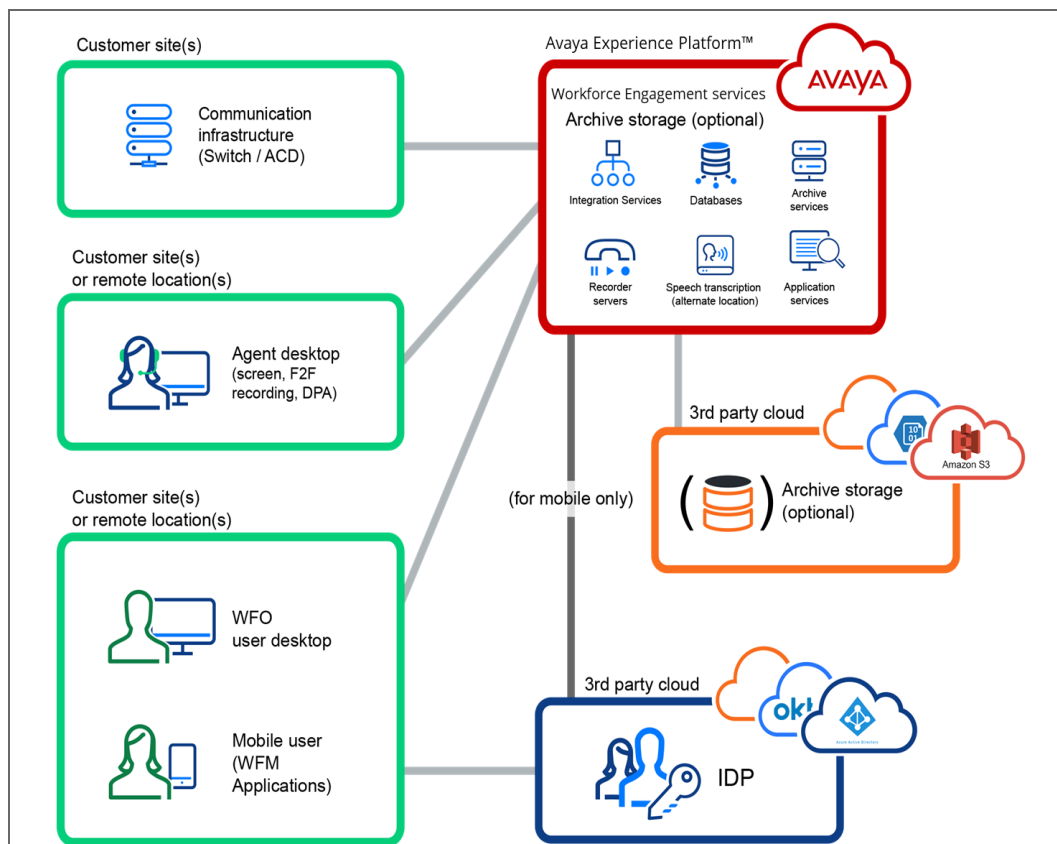
Avaya Experience Platform™ Workforce Engagement connectivity

In cloud deployments, the communication infrastructure communicates with Avaya Experience Platform™ Workforce Engagement.

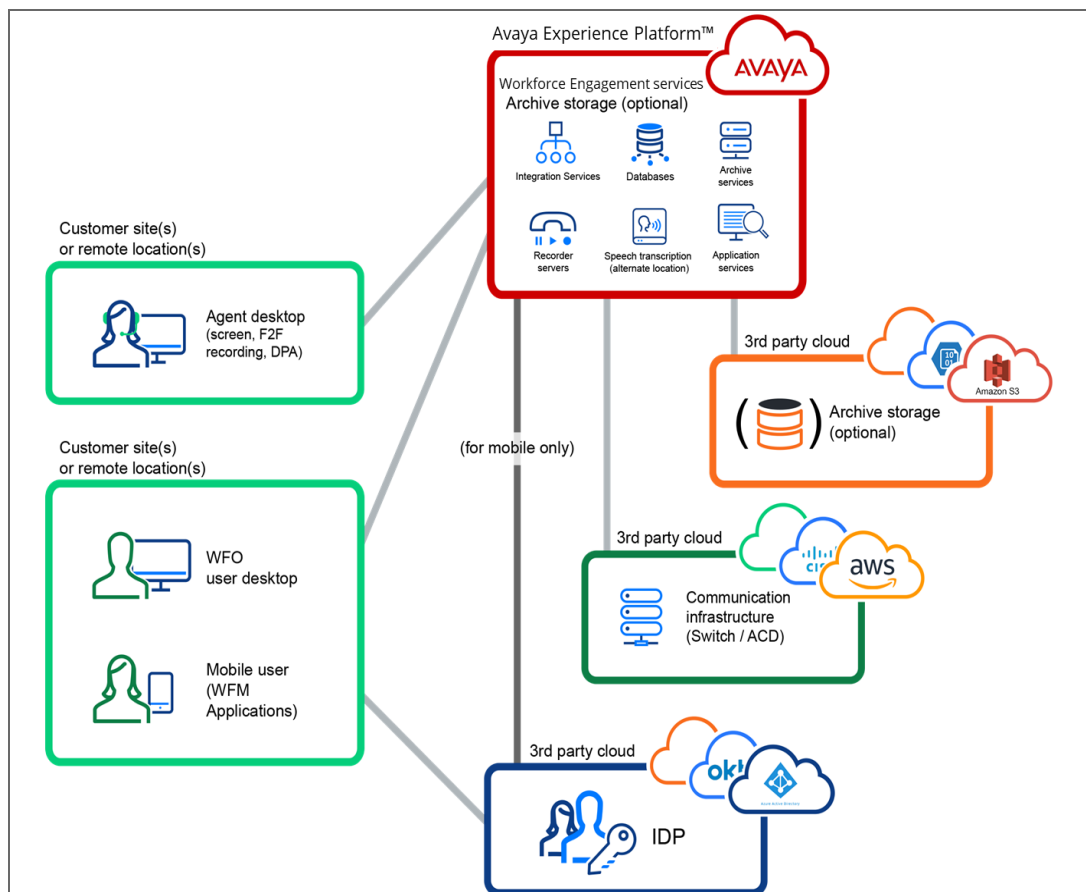
The communication is as follows:

- Recording solutions requiring high Quality of Service (QoS) delivery, typically require AWS Direct Connect (DX) for voice and video recording.
You can use VPN as an alternative delivery method to DX, based on cost performance considerations. As connectivity over internet does not guarantee consistent network performance, some recorded interactions may be of lower quality with a VPN connection.
- For recording solution with specific cloud-based communication infrastructures, such as Amazon Connect and MS Teams, the service provider is responsible for the connection to Avaya Experience Platform™ Workforce Engagement.
- Other types of communication use encrypted channels going over the open internet, or encrypted tunnels (VPN), depending on the customer's requirements.
- Communication between desktops, mobile devices, archive storage, and IdP, with Avaya Experience Platform™ Workforce Engagement uses encrypted channels going over the open internet.

On-premises communication infrastructure



Cloud-based communication infrastructure



Related topics

[Network connectivity](#), page 13

Networking in cloud deployments

The Avaya Experience Platform™ Workforce Engagement supports various networking configurations to provide secure communication, and to support a secure and robust architecture.

Topics

Network connectivity13

Network security15

Bandwidth, latency, ports, and connection types16

Network connectivity

The Avaya Experience Platform™ Workforce Engagement solution requires connections between the customer resources and the cloud. It is the responsibility of both the service provider and the customer to manage these connections.

The customer must provide one or more of the connectivity options, according to the connection requirements: AWS Direct Connect, VPN, or TLS.



For connections where we specify TLS, these can flow over the internet, over AWS Direct Connect, or be encapsulated in a VPN connection.

For connections where we specify requiring VPN, these can be encapsulated in a VPN connection, or over AWS Direct Connect.

Transport Layer Security (TLS) connection

Transport Layer Security (TLS) is an encrypted network communication protocol designed to provide communication security over the public internet, and as such, uses public IP addresses to connect. Access by others is blocked through the encryption of data.

TLS provides:

- **Authentication:** The identity of the communicating parties is authenticated using public-key cryptography. This authentication is generally required for at least one of the parties (typically the server).
- **Data integrity:** The connection is reliable because each message transmitted includes a message integrity check using a message authentication code to prevent undetected loss or alteration of the data during transmission.

Virtual private network (VPN) connection

Virtual private network (VPN) is an encrypted connection over the public internet, extending the customer's existing security and management policies to the cloud, as if they are running within their own infrastructure.

Site-to-cloud VPN is provided using **Aviatrix Site2Cloud**, where the customer's firewall appliances are utilized on the customer site, and virtual Aviatrix gateway instances are utilized on the Cloud.

AWS Direct Connect (DX) connection

AWS Direct Connect (DX) is a networking service used to access AWS cloud services over a dedicated connection with consistent network performance. It is an alternative to using the internet to access AWS cloud services, and is well suited for recording streaming voice and video.

With DX, a connection is established between a DX peering location and the Avaya Experience Platform™ Workforce Engagement. The customers are responsible to establish their own high quality connection to the DX peering location.

DX is available at locations around the world. In some campus settings, DX is accessible using a standard cross-connect operated by the same provider. Customers that do not have equipment at a DX location, can access DX with partners assistance, such as of a member of the AWS Partner Network.

Network Address Translation (NAT)

The system supports Network Address Translation (NAT).

NAT is not supported for audio recording media traffic between the customer communication infrastructure and cloud capture modules. NAT support for signalling traffic between the customer communication infrastructure and cloud capture modules is vendor specific.

Related topics

[Bandwidth, latency, ports, and connection types](#), page 16

Network security

Avaya Experience Platform™ Workforce Engagement requires full TLS for all participating end points such as desktops, mobile devices, Avaya Experience Platform™ Workforce Engagement , and 3rd party cloud. It is the responsibility of the customer to provide and maintain TLS certificates, to ensure secure communication.

TLS certificates responsibilities

The customer is responsible for generating TLS certificates according to the industry standards. The customer is also responsible for:

- **Tracking:** Ensuring the customer is aware of expiry dates of TLS certificates on all end-point.
- **Renewing:** Creating or acquiring renewed certificates for all end-point.
- **Installing:** Installing all renewed certificates on all end-points.

Server	TLS Certificate Type	Responsible for first install	Responsible for renewal
Desktops and mobile devices	CA Certificates	Customer	Customer
Communication infrastructure (switch/ACD)	Server Certificate	Customer	Customer
IdP (for SAML and OIDC)	Server Certificate	Customer	Customer (See note)
Archive storage	Server Certificate	Customer	Customer



If the customer is using Azure AD to integrate with VCP Identity, they have no need to track or maintain SAML certificates.



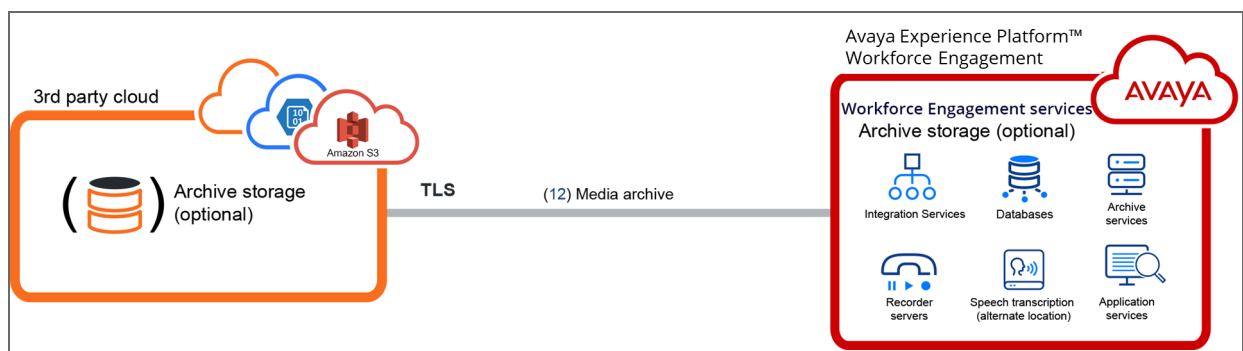
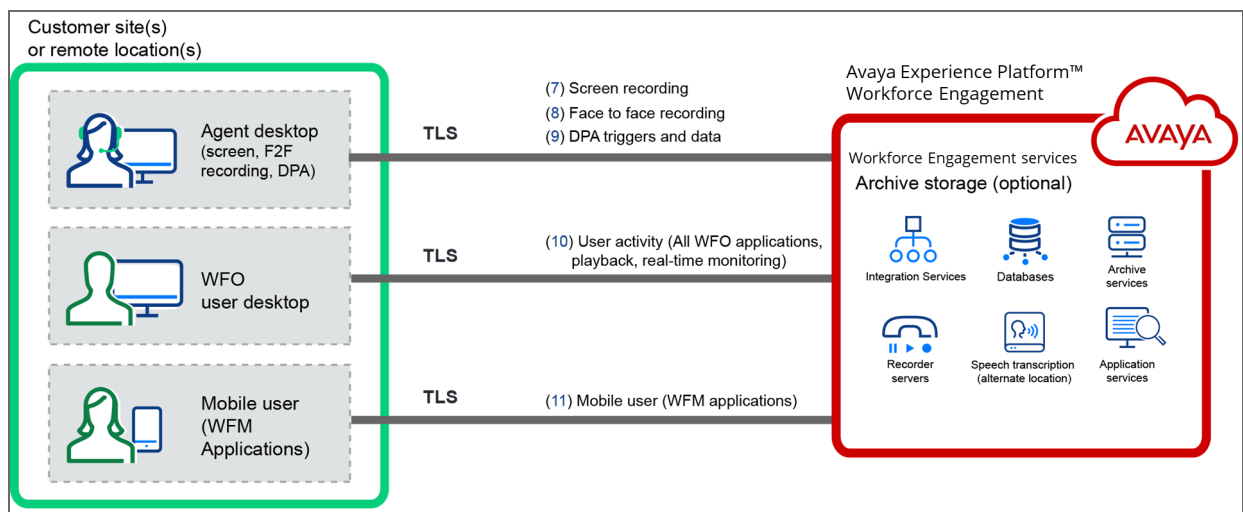
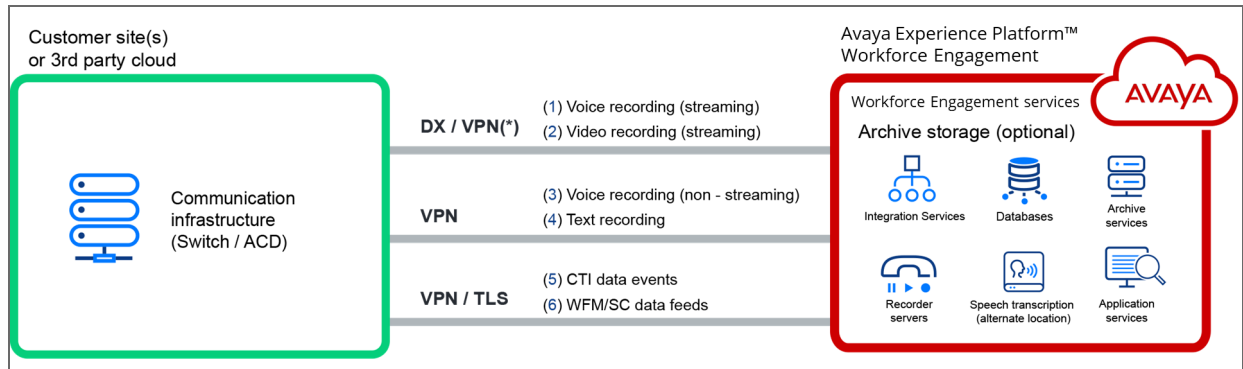
The customer must provide server certificate only if the server is customer supplied and not Service Provider supplied.

Mobile devices

In addition to deploying TLS server certificates, root CA certificates need to be installed on all end-user devices. When public CA is used, the root CA certificate is typically already installed in the trusted root CA store on the device, which simplifies the deployment. In case the customer's private Certificate Authority is used, root CA certificates need to be distributed to mobile devices (typically using MDM).

Bandwidth, latency, ports, and connection types

The cloud deployment data flows show the way information flows between components in different locations, with the required connection type. Bandwidth and port requirements depend on the data flow.



* The following connection types are required:

- For streamed voice and video recording:
 - Recording solutions requiring high Quality of Service (QoS) delivery typically require AWS Direct Connect (DX).
 - You can use VPN connection as an alternative delivery method to DX, based on cost performance considerations. As connectivity over internet does not guarantee consistent network performance, some recorded interactions may be of lower quality with a VPN connection.
 - For Amazon and MS Teams recording, the service provider is responsible for providing the connection between the recording source and SaaS Cloud.
- If DX is used for media recording purposes, use DX connection for CTI data events and WFM/SC data feeds as well.

If DX connection is not required, the CTI data events and WFM/SC data feeds require a VPN connection. Exceptions are Amazon Connect and Twilio integrations, where TLS connection can be used.

Related topics

[Bandwidth and latency requirements](#), page 17

[Port requirements](#), page 20

Bandwidth and latency requirements

The customer-specific bandwidth requirements are provided in the Customer Furnished Equipment Guide.

Quality of Service (QoS) is a measurement of the latency between the various resources within each deployment model.

Bandwidth requirements for typical scenarios, and latency requirements

# in diagram	Data flow	Bandwidth example	Latency round trip time (RTT)
1	Voice recording (streaming)	8.08 Mbps for 100 concurrent agents, G.729A stereo. Use this calculator for more options: https://www.bandcalc.com	200ms NOTE: Higher latencies can be supported, however tolerance for packet loss and out of sequence packet errors is reduced, and recording can be affected.

# in diagram	Data flow	Bandwidth example	Latency round trip time (RTT)
2	Video recording (streaming)	Consult your service provider representative	200ms NOTE: Higher latencies can be supported, however tolerance for packet loss and out of sequence packet errors is reduced, and recording can be affected.
3	Voice recording (non-streaming)	Consult your service provider representative	N/A
4	Text recording	Consult your service provider representative	N/A
5	CTI data events	0.01 Mbps for 1000 calls per hour	130 ms
6	WFM/SC data feeds	negligible	N/A
7	Screen recording	Minimum for 100 concurrent agents using single monitor: <ul style="list-style-type: none"> • 5.60 Mbps with color reduction • 23.80 Mbps with rich color Minimum for single at-home agent using single monitor: <ul style="list-style-type: none"> • 0.06 Mbps with color reduction • 0.25 Mbps with rich color Actual bandwidth can vary depending on the screen activity, and resolution.	N/A
8	Face to face recording	Consult your service provide representative	N/A
9	DPA triggers and data	0.06 Mbps for 100 concurrent agents	

# in diagram	Data flow	Bandwidth example	Latency round trip time (RTT)
10	WFO desktop user activity (all WFO user applications, playback, and real-time monitoring)	See table below for information (*)	Network delay higher than 150 ms can cause delays in the response time
11	Mobile user	3 Mbps for one mobile user	Network delay higher than 150 ms can cause delays in the response time
12	Media archived	1.77 Mbps for audio archiving at 1000 interactions per hour, 3 minutes per call, G.729A mono	N/A

* Bandwidth requirements for WFO desktop user activity

WFO desktop user activity bandwidth includes all WFO user applications, playback, and real-time monitoring. It does not include screen recording, face-to-face recording, and DPA, which are calculated separately.

Assumptions

- Usage profile assumes a ratio of 1:10 supervisors to agents.
- G.729 stereo.
- For 1000 employees, 4 concurrent downloads, 20 concurrent continuous playbacks or RTM sessions.

WFO bandwidth from Data Center to desktop when the recorders are on the Data Center

Use	WFO applications + audio playback/RTM	WFO applications + audio playback/RTM + reduced screen playback/RTM	WFO applications + audio playback/RTM + rich screen playback/RTM
Single user	3 Mbps	24 Mbps	100 Mbps
1000 employees	60 Mbps – peak (required) 10 Mbps – sustained	120 Mbps	500 Mbps

WFO bandwidth from Data Center to desktop when the recorders are on the site

Use	Audio playback/RTM	Audio playback/RTM + reduced screen playback/RTM	Audio playback/RTM + rich screen playback/RTM
Single user	0.6 Mbps	24 Mbps	100 Mbps
100 employees	3 Mbps (required) <ul style="list-style-type: none"> • 2.4 Mbps download • 0.6 Mbps continuous/RTM 	120 Mbps (required) <ul style="list-style-type: none"> • 96 Mbps download • 24 Mbps continuous/RTM 	500 Mbps (required) <ul style="list-style-type: none"> • 400 Mbps download • 100 Mbps continuous

Related topics

[Bandwidth, latency, ports, and connection types](#), page 16

Related information

Customer Furnished Equipment (CFE)

Port requirements

The customer must adhere to the ports requirements to enable communication through firewalls.

# in diagram	Data flow	Source	Destination	Port	Comments
1,2,3,4	Voice, Video, Text recording				See the <i>Cloud Firewall Ports Configuration Guide</i>
5	CTI data events				See the <i>Cloud Firewall Ports Configuration Guide</i> for integration-specific ports
6	WFM/SC data feeds				See the <i>Cloud Firewall Ports Configuration Guide</i> for integration-specific ports

# in diagram	Data flow	Source	Destination	Port	Comments
7	Screen recording	Agent desktop	Avaya Experience Platform™ Workforce Engagement	WSS (29434), HTTPS (29436)	
8	Face to face recording	Agent desktop	Avaya Experience Platform™ Workforce Engagement	HTTPS (443)	
9	DPA triggers and data	Agent desktop	Avaya Experience Platform™ Workforce Engagement	DPA data HTTPS (443) DPA triggers HTTPS (3020)	
10	WFO user activity	WFO user desktop	Avaya Experience Platform™ Workforce Engagement	HTTPS (443)	
11	Mobile user (WFM apps)	Mobile	Avaya Experience Platform™ Workforce Engagement	HTTPS (443)	
12	Media archive	Avaya Experience Platform™ Workforce Engagement	3rd part cloud (AWS S3, Azure Blob Storage)	HTTPS (443)	

Related topics

[Bandwidth, latency, ports, and connection types](#), page 16

Related information

Cloud Firewall Ports Configuration guide

User authentication in cloud deployments

User authentication is the process in which it is verified that users attempting to sign in to applications, are allowed to do so. This can be accomplished through various authentication methods. After confirming the user identity, that identity is used to determine the appropriate access rights of the user.

Topics

User authentication methods	23
DB Realm customer requirements	25
SAML customer requirements	26
OpenID Connect for mobile customer requirements	27

User authentication methods

Several methods of user authentication are supported. These include DB Realm, Security Assertion Markup Language (SAML), and OpenID Connect (OIDC). Each method uses a specific authentication principle (federated or form based), and can be used for specific applications (desktop/web, mobile, reports).

DB Authentication (DBRealm)

The DB Realm is a Form-based authentication method. DBRealm authenticates the user with a user name and password that is maintained solely within the cloud credentials store. The password hashes are managed securely in the credentials store. When DB Realm authentication method is used, password and account locking policies are also managed within the cloud.

Security Assertion Markup Language (SAML)

SAML is a Federated authentication method, which uses XMLs for exchanging user authentication between the customer identity provider (IdP) and WFO as the Service Provider (SP), or Relying Party (RP). SAML SSO works by transferring the user's identity from the IdP to SP. This is done through an exchange of digitally signed XML documents (SAML assertion).

OpenID Connect (OIDC) for mobile

OpenID Connect is a Federated authentication method, and a standard for single sign-on and identity provision on the internet. Similar to SAML, OIDC is an authentication method where the user's credentials are held with a third-party identity provider (IdP) and not within the cloud. The user's identity is verified based on a simple JSON- based identity token. This is delivered on top of the OAuth protocol and is suitable for mobile applications, such as Verint WorkView.

Related topics

[User authentication principles](#), page 23

[User authentication matrix](#), page 24

[SAML customer requirements](#), page 26

[DB Realm customer requirements](#), page 25

[OpenID Connect for mobile customer requirements](#), page 27

User authentication principles

Several authentication principles are supported. Once you decide on the principle and the applications to support, you can determine the authentication method.

The following authentication principles are supported:

- **Form-based authentication:** User credentials are provided in a WFO sign in form, which is sent to WFO, and the user is then authenticated against the credentials store.
If form based authentication method is selected, using HTTPS protects user credentials.
- **Federated authentication:** User credentials are held by a third-party identity provider and a token is provided to WFO to validate.

Related topics[User authentication methods](#), page 23

User authentication matrix

Determine the authentication method to use based on the applications you use, and your organization's user authentication policy. You can use a mixture of mechanisms, for example SAML for Desktop/Web and DBRealm for Ad hoc reports.

Authentication Method	Authentication Principle	Desktop/Web	Ad hoc Reports	Mobile
DB Authentication (DBRealm)	Form-Based Authentication. Credentials validated against the cloud credentials store.	✓	✓	✓
Security Assertion Markup Language (SAML)	Federated Authentication	✓	✗	✗
OpenID Connect (OIDC)	Federated Authentication	✗	✗	✓

Related topics[User authentication methods](#), page 23

DB Realm customer requirements

The DB Realm authentication method authenticates the user with a user name and password that is maintained solely within the cloud credentials store. The password hashes are managed securely in the credentials store. When DB Realm authentication method is used, password and account locking policies are also managed within the cloud.

User Identifier

User identifier attribute is required with the DB Realm authentication.

The same value used as the User identifier must then be configured in the **Username** field in WFO (User Management > Security > Usernames workspace).

SAML customer requirements

Configuring SAML is done by registering WFO Desktop/Web applications with the IdP. The Identity Provider (IdP) holds the user's credentials.

User Identifier

A User Identifier is required, to identify the user during authentication.

Use any attribute as the subject of the assertion. For example, use the User-Principal-Name as the **Name ID** attribute in the ADFS IdP.

The same value used as the User identifier must then be configured in the **Username** field in WFO (User Management > Security > Usernames workspace).

In a multi-tenant environment, for uniqueness, use email format as the **Username**.

Clock skew

SP signature is invalid if the **NotBefore** field in the SAML request does not match the IdP clock skew policy.

For example, if a request arrives to ADFS that does not match its clock skew policy, the ADFS declines the request. To change the default ADFS policy to 2 minutes for example, run the following command to override the default policy and set the **NotBefore** value back 2 minutes before the ticket is created:

```
Set-ADFSRelyingPartyTrust -TargetIdentifier "urn:party:sso" -NotBeforeSkew 2
```

Where "urn:party:sso" is the Identifiers of your SP

WFO SP relying party in the IdP

Configure the WFO SP relying party in the IdP by importing the SP metadata XML you received from the service provider. The metadata is exported from WFO as part of the deployment procedure.

In your IdP, select the authentication methods. For example, select **Forms Authentication** and **Certificate Authentication** methods in an environment that supports both.

IdP SAML metadata

IdP SAML metadata XML file is required for configuring the Weblogic Identity Provider settings. Provide the IdP SAML metadata XML file to the service provider.

Exchanging the metadata is done manually as part of the configuration procedure. Automatic exchange of metadata is not supported.

When changing the IdP properties, it is required to re-send the new IdP-initiated metadata to the service provider.

Desktop applications URL

Configure desktop applications with the signin URL based on the signin type: SP-initiated (default), or Idp-initiated. For the Idp-initiated URL, see Desktop Applications Deployment Reference and Installation Guide.

Related information

Application configuration updates (*Desktop Applications Deployment Reference and Installation Guide*)

OpenID Connect for mobile customer requirements

Configure Open ID Connect for the Verint mobile applications by registering it with the IdP, retrieving an application ID, and entering this ID into the cloud.

The Identity Provider (IdP) holds the credentials of the user. The IdP is a third-party solution which must be supported to work with the cloud. The following IdPs are supported:

- Azure AD
- ADFS
- Google
- Okta
- PingFederate
- OneLogin
- Auth0

Configure the IdP to recognize one or more of the Verint mobile applications as registered applications.

User Identifier

A User Identifier is required to identify the user during authentication.

In OIDC, the Mobile application authenticates itself against WFO using an **OIDC idToken**. The **OIDC idToken** is received from the IdP, following successful sign-in to the IdP. This token contains the user name, and other information used by WFO to validate the token. WFO uses user name in the token for authentication.

Identify the attribute (aka claim) included in the **OIDC idToken** that holds the user name to authenticate (for example, email, sub, or upn). This attribute is then configured as the **user name Claim** in the Feature Settings window, under Mobile Authentication Method.

The user name value provided by the IdP must be identical to the user name value defined in WFO (**user name** field in User Management > Security > Usernames workspace). This value must be included in the **OIDC idToken** as the user name attribute value.

In a multi-tenant environment, for uniqueness, use email format as the user name.

If the actual user name used to authenticate with the IdP is different from the user name configured in WFO, the **OIDC idToken** must include the WFO user name. For example, if you use your email to authenticate with the IdP, while your user name configured in WFO is your **sAMAccountName**, the user name attribute identified in the **OIDC idToken** must contain the **sAMAccountName**.

Security

The mobile OIDC implementation uses Proof Key for Code Exchange (PKCE) mechanism. The mechanism is used to validate client and server authenticity, and reduce the chances of successful "Authorization Code Interception Attack". Select this option when registering the Verint mobile applications with the IdP.

client_secret (embedded secret in source code) is not supported and is considered less secured.

Verint mobile applications registration with the IdP

Customers are required to create their own accounts where the user names created must match the user names used in WFO. This process ensures that the WFO roles and privileges of the users are mapped properly when the user signs into the mobile application.

Customers are required to register the native Verint mobile applications with their IdP.

If required during the registration process, the following details are useful:

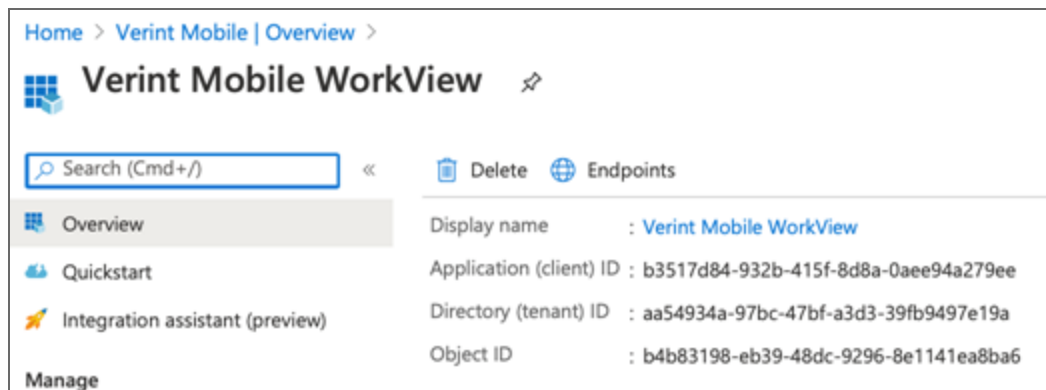
- Name: mobile application name, such as **Verint WorkView**, or **Verint TeamView**
- Application type: **Native**
- Bundle ID: **com.verint.workview**, or **com.verint.teamview**
- Redirect URI: **com.verint.workview://oauthredirect**, or **com.verint.teamview://oauthredirect**

Example: Register Verint WorkView with Azure AD as the IdP

In this example, you are required to sign in to the Azure AD portal as an owner, and fill in the form.

The screenshot shows the 'Register an application' page in the Azure AD portal. The breadcrumb navigation is 'Home > Verint Mobile | App registrations >'. The title is 'Register an application'. There is a red asterisk next to the 'Name' field, which is labeled 'Name'. Below it, a description says 'The user-facing display name for this application (this can be changed later)'. The input field contains 'Verint Mobile WorkView' and has a green checkmark on the right. Below this is the 'Supported account types' section. Under the heading 'Who can use this application or access this API?', there are three radio button options: 'Accounts in this organizational directory only (Verint Mobile only - Single tenant)' (selected), 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', and 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)'. A link 'Help me choose...' is below the radio buttons. The 'Redirect URI (optional)' section follows, with a description: 'We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.' The 'Redirect URI' field has a dropdown menu set to 'Public client/native (mobile ...)' and an input field containing 'com.verint.workview://oauthredirect' with a green checkmark on the right.

Azure AD assigns the application a unique client identifier, the Application ID. You need this ID for the next step.



Related information

<https://docs.microsoft.com/en-us/azure/active-directory/active-directory-app-registration>

If this link does not work, search for Azure AD application registration.

Archiving in cloud deployments

Archive provides a flexible and secure service for managing the long-term storage of recorded media and associated metadata. Archive also manages the retention of the data to meet regulatory and enterprise requirements. Archive supports common cloud storage devices, and the customer is required to provide information relating to these devices. Archive storage can be deployed on-premises, on the Avaya Experience Platform™ Workforce Engagement, or on a 3rd party cloud.

Topics

Supported archive devices31

Fixed media definition fields32

Supported archive devices

The following table lists supported devices.

Device
Amazon S3 for native Amazon cloud storage
Amazon S3 for other cloud storage devices such as IBM Storage Object, Dell ECS
Azure Blob Storage
GCS (Google Cloud Storage)

Fixed media definition fields



The Archive Media definition fields provide connection information for the fixed media that is used for archiving the recorded content.

The following table lists the information that you need to have available.



For IBM Storage Object or Dell ECS, you use Amazon S3 V2.

Archive Media Amazon S3 media type

Field	Description
AWS Signature Version	The authentication mode: V2 (AWS Signature Version 2) or V4 (AWS Signature Version 4).
Bucket Name	The Amazon S3 bucket (or vault) name. The name is provided at the time a user requests a new bucket. In some implementations, the term bucket and vault are synonymous.
	 S3 buckets with Object Lock enabled are not supported.
Authentication Type	<p>When AWS Signature Version 4 is selected, you can choose the authentication type to use: Access Key or Role.</p> <p>When AWS Signature Version 2 is selected, Access Key is the only authentication type allowed.</p>
Access Key ID	Needed when Access Key is used as the Authentication Type. Access Key of the identity you are using to send the archiving request.
Secret Access Key	Needed when Access Key is used as the Authentication Type. The S3 Access Key is used to calculate the signature of an archiving request.
Role Name	<p>Needed when Role is used as the Authentication Type. Name of the IAM role used to authenticate access to the media.</p> <p>  The role must have a trust relationship with an IAM user that has the AssumeRole policy attached. </p>
External ID	Needed when Role is used as the Authentication Type.

Archive Media Azure Blob Storage media type

Field	Description
Account Name	Name of the storage account from portal.azure.com. Value is 3–24 characters.
Account Key	Access key to use to authenticate the recorder when making requests to the storage account. The 108-character key is available in the Azure Portal at Settings/Access keys.
Container Name	Name of the container in which to archive. Maximum 63 characters.
Endpoint Protocol	Protocol to use for the connection, http or https (recommended).
Endpoint Suffix	A valid URI suffix, such as <i>core.windows.net</i> (16 characters), to use to establish the connection to storage services. Maximum 26 characters.

Archive Media Google Cloud Storage media type

Field	Description
Bucket Name	<p>The GCS bucket name to which interactions are exported. Buckets are the basic GCS containers that hold data. Everything stored in GCS must be contained in a bucket. You can use buckets to organize data and control access to data, but unlike directories and folders, you cannot nest buckets.</p> <ul style="list-style-type: none">• Bucket names can only contain lower-case letters, numeric characters, dashes (-), underscores (_), and dots (.). Spaces are not allowed.• Bucket names must start and end with a number or letter.• Bucket names must contain from 3 to 63 characters. Names containing dots can contain up to 222 characters, but each dot-separated component can be no longer than 63 characters.• Bucket names cannot be represented as an IP address in dotted-decimal notation (for example, 192.168.5.4).• Bucket names cannot contain "google" or the prefix "goog".

Field	Description
Authentication Type	<p>You can choose between two authentication types: Service account authentication or Implicit authentication.</p> <ul style="list-style-type: none"> • Service account authentication - Provides accessing of private data on behalf of a service account outside Google cloud environments. To use this authentication, you must create a Google cloud platform service account and download its private key as a JSON file. A client passes the JSON file to Google Cloud Client Libraries to authenticate at run time. • Implicit authentication - Provides accessing of private data on behalf of a service account inside Google Cloud environments. <p>With this authentication type, when an application runs inside a Google cloud environment, the application uses the service account provided by the environment. Google Cloud Client Libraries automatically find and use the service account credentials by using the GOOGLE_APPLICATION_CREDENTIALS environment variable.</p>
Private Key	<p>This field is used only when Service account is selected as the Authentication Type. This private key is a JSON file that is required for service account authentication.</p> <p>The private key (JSON file) can be created and downloaded from a Google Cloud Platform service account.</p>
Impersonate	<p>Select this option if you want to allow a user(s) to authenticate into the system using the Google Cloud Platform service account that is specified in the Target principal field. Typically, the service account that is impersonated (specified in the Target principal field) has greater access to the system than the service accounts associated with individual users.</p> <p>For example, you can have an account set up that has full access to the system that exists to support impersonation. A user can log in using their own account, and if impersonation is configured for that user, the user is granted full access to the system.</p> <p>To configure impersonation for a user, the user must have their account specified in the service account that is impersonated. Users whose accounts are not specified in the service account that is impersonated cannot use this feature.</p> <p>Impersonation is a security feature that allows you to limit high-level access to the system to a few selected users.</p>
Target principal	<p>This field is used only when the Impersonate option is selected. This field specifies the service account that is impersonated. To specify the service account that is impersonated, enter the email address found in that service account in this field.</p>

Client application management

Desktop and mobile applications are the responsibility of the customer.

Topics

Desktop applications36

Mobile applications38

Desktop applications

Desktop applications are client applications installed on employee desktops to facilitate users to perform their role within the enterprise.

It is the responsibility of the customer to install and manage all desktop applications.

Related topics

[Desktop antivirus requirements](#), page 36

Related information

Desktop Applications Deployment Reference and Installation Guide

Desktop antivirus requirements

Antivirus applications scan for viruses periodically or as part of real-time protection.

The customer is required to customize antivirus scan criteria to exclude specific types of files and folders. Doing this improves performance, and helps ensure that files are not locked when attempting to access them.

Use the exclusion list to set up your antivirus exclusions. The exclusion list refers to both real-time protection and periodical virus scans.

Desktop Exclusion List

Folder	Exclusion list
%PROGRAMFILES%\AvayaAura\DPA\Client	Exclude all files and subfolders, or the process DCUApp.exe.
%PROGRAMDATA%\AvayaAura\DPA\Data	Exclude all files and subfolders, or the process DCUApp.exe. Exclude the following typical file extensions at a minimum: *.svn, *.htm, *.sxn, *.ini, *.def, *.pds, *.xml, *.bmp, *.txt
%PROGRAMFILES%\AvayaAura\CaptureService	Exclude all files and subfolders, or the process CaptureService.exe.
%PROGRAMFILES%\AvayaAura\Media Storage Directory	For Face-to-Face Voice Interaction Recording, exclude this folder and all files and subfolders.

Notes on antivirus exclusions for Desktop and Process Analytics (DPA)

- Antivirus applications lock files when scanning. If DPA attempts to write to a locked file, or attempts to delete, rename, or move a locked file, it fails.
- DPA uses operating system hooking to detect key presses to determine when a machine is idle. It also uses operating system hooking to detect mouse clicks to fire click triggers. Because malware or virus-like programs can use operating system-level hooking to perform keylogging, antivirus applications determine that DPA has key logging characteristics, and they remove the affected component dlls.
- DCUApp.exe forcibly opens and keeps open several client files on disk to prevent users from renaming, deleting, or modifying them. Locking files in this manner can prevent antivirus applications from determining their content and result in DCUApp.exe being marked as suspect.
- DPA needs to update .ini file for configurations, .xml files for triggers and create .log /.txt files for tracing. Not having the exclusions in place can prevent the read/write required on the 'programdata' directory, which can cause triggers not to be added to file and therefore not fire in user session.
- Files with the stated extensions are in the DPA data directory and are locked "open" by DCUApp to prevent user intrusion. They also change in size as and when configuration updates occur. Antivirus heuristic algorithms treat files which are locked and change in size as potential virus payload files.

Mobile applications

The Verint mobile apps enable employees, supervisors, and managers to easily access their information from their mobile devices. The mobile apps are available in the public stores (Apple Store and Google Play).

The customer is required to manage mobile devices using Enterprise Mobility Management (EMM) solutions. EMM refers to the collection of systems and processes connecting mobile devices to the enterprise infrastructure and workflows.

The customer is required to:

- Verify that end users have access to the mobile apps they need to do their work
- Manage the apps on both company devices, and personal devices of the users
- Verify that the network and data remain secure
- Use a solution that supports distribution of mobile apps from the public store (Google Play and Apple Store).

Related topics

[Applications](#), page 38

[Mobile device management](#), page 38

Applications

Work View and Team View mobile apps allow employees, supervisors, and managers to quickly, and easily log on to their information from an iOS or Android device.

- **Verint Mobile Work View (for employees)**

Work View allows employees to view and manage their schedule, view their performance scorecards, and stay up-to-date with notifications and updates.

- **Verint Team Mobile View (for supervisors and managers)**

Team View allows supervisors and managers to view their employees' schedules, manage their employees' requests, and stay up-to-date with notifications.

After the mobile apps sign in process, employees, supervisors, and managers are able to receive push notifications to their mobile devices. For example, supervisors receive push notifications when their employees' schedule changes or their shift bidding status changes.

Mobile device management

Mobile devices are managed using Enterprise Mobility Management (EMM). EMM refers to the collection of systems and processes connecting mobile devices to the enterprise infrastructure and workflows.

The core elements of EMM suites are:

- **Mobile Device Management (MDM):** Tools used for mobile device administration and policy enforcement at the device level, such as rooted device/jailbreak detection, OS configuration management, device tracking, remote wiping of devices, and network access (VPN, WiFi).
- **Mobile Application Management (MAM):** Administration at the individual application level, such as application distribution to mobile devices, version management, performance monitoring, application wrapping, etc.
- **Mobile Identity Management (MIM):** Tools providing Identity and Access Management functions for mobile devices, such as user authentication, device certificates, and behavioral and contextual access (for example, according to how the device is used and from where).

The use of EMM tools enhances overall security and facilitates administration tasks.

Examples of how EMM tools can be useful:

- Route all mobile network access through an EMM gateway. This solution allows for monitoring and fine-tuning access decisions before accessing the internal network. For example, access can be restricted according to device properties, specific apps, network location, or specific users.
- Multi-Factor Authentication (MFA) is achieved by enforcing strong authentication using MDM, MAM, or MIM.
- Enforce device password protection to encrypt all device content when locked.
- If a private Certificate Authority is used, use MDM to distribute root CA certificates to mobile devices.
- Remote wiping of devices using MDM, or of application data using MAM (for data saved on mobile devices).

EMM gateway controlling access of mobile devices to load balancer in DMZ

