



Avaya Experience Platform™ Workforce Engagement

Desktop Applications Deployment Reference
and Installation 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	9
Getting started	13
Desktop Applications installation workflow	14
Desktop Applications update policy	15
Desktop Applications matrix	16
Obtain the installation packages	18
Customer requirements	19
Operating systems	20
Supported operating systems	20
Windows security settings	20
Elevate UAC security	21
Windows firewalls	21
Antivirus settings	21
Thin clients and VMware	22
Hardware specifications	25
Browser Settings	26
General Chrome settings	26
Configure workstations in TLS environment	28
Install Root CA certificates on workstations	28
Third-party software required by desktop applications	30
Third-party software required for browsing	32
Localization	33
Folder permissions	34
Installation by role: silent distribution	36
Silent distribution guidelines	37
Before you begin a silent distribution	37
Silent distribution workflow	37
Silent distribution for agents	39
Desktop Applications for agents	39
Example script for agents	39
Silent distribution for supervisors/managers	41
Desktop applications for supervisors/managers	41
Example script for supervisor/manager	41
Silent distribution for administrators and analysts	43
Desktop applications for administrators and analysts	43

Example script for administrators and analysts	43
Installation by application	46
Desktop Resources	47
Install Desktop Resources manually	47
Desktop Resources silent install parameters	48
Generate an Internal API Key	48
Desktop Supportability	50
Install Desktop Supportability	50
Desktop Messaging	51
Workflow: Install Desktop Messaging manually	51
Install Desktop Connection Manager manually	51
Install Desktop Messaging manually	53
Install Desktop Messaging by silent distribution	53
Desktop Messaging silent install parameters	54
Uninstall Desktop Messaging manually	55
Uninstall Desktop Messaging silently	56
Desktop and Process Analytics (DPA) clients	57
Install the DPA client manually	57
DPA client configuration information	58
Configure DPA Data Transfer service user name and password	59
Install DPA client by silent distribution	60
Add 'Install As' option	60
DPA client silent distribution script examples	61
DPA client silent script distribution parameters	61
DPA installation in third-party environments	62
Install the DPA client for citrix and terminal servers	63
Citrix published applications	64
DPA client on remote environment deployment	64
DPA client Installation on a Virtual Desktop Infrastructure (VDI)	65
DPA client installation on other virtual environments	65
DPA client installation in Microsoft AppV	65
Verify DPA monitoring	66
DPA integration with various application types	66
Enable DPA to trigger on Terminal Emulators	67
Enable DPA to trigger events on web browsers	68
Enable DPA event triggers in Google Chrome	69
Enable DPA Validator to capture Google Chrome screens	69
Enable DPA window triggers in Mozilla Firefox	70
Enable DPA in Java applications	71
Enable DPA in SAPLOGON/SAPLOGON applications	71
Enable DPA integration in Kana web applications	71

DPA public-private token authentication	71
Prepare DPA authentication keys	72
Modify DPA authentication keys	74
Uninstall/rollback DPA clients	74
Uninstall and rollback DPA client using the original msi	75
Uninstall and rollback DPA clients using a script	75
Uninstall a DPA client through add/remove programs	76
Install DPA Validator	76
DPA Process Discovery	78
Install Process Discovery	78
Add Process Discovery Menu to Microsoft Office Visio	79
Process Discovery silent install parameters	79
Form Designer	81
Install Form Designer manually	81
Form Designer silent install parameters	82
Logger	84
Install Logger manually	84
Logger silent install parameters	85
Player	86
Install the Plugin Player manually	86
Silent install parameters for Plugin Player	89
Playback without Portal	90
Enable real time playback of encrypted screen content in transit	91
Configure stereo recorded contact playback as mono	91
Enable stereo playback as mono	91
Disable stereo playback as mono	92
Configure volume amplification	93
Enable volume amplification	93
Disable volume amplification	94
Video playback tuning	94
Configure network adapters for real-time audio playback in plugin Player	95
Configure the Player to improve screen playback performance	96
Phonetics Boosting	97
Install Phonetics Boosting manually	97
Screen Capture and AIM	99
Install Screen Capture and AIM manually	99
Configure Screen Capture and AIM in a Citrix environment	102
Configure Screen Capture and AIM in a VMware Horizon environment	103
Screen Capture and AIM post installation notes	103
Screen Capture and AIM silent install parameters	104
Screen Capture basic install parameters	104
AIM silent install parameters	107

Terminal Services Server silent install parameters	110
Strategic Planner Client	112
Install Strategic Planner manually	112
Configure the license key for Desktops	113
Configure the license key for Citrix	113
Strategic Planner silent install parameters	114
Face to Face Voice Interaction Recording	115
Advanced administration for desktop applications	116
Application configuration updates	117
Modifying desktop computer name	117
Application Load Balancer name change	117
Update desktop application configuration files	118
Playback configuration	118
Form Designer configuration	119
Desktop and Processing Analytics (DPA) configuration	120
Desktop Messaging configuration	120
DPA Process Discovery configuration	120
Strategic Planner configuration	120
Phonetic Boosting configuration	123
Upgrade legacy desktop applications	124
Upgrade V15.1 workstations	125
Silent uninstall	126
DPA client upgrade	128
Transition to TLS	129
Screen Capture module and AIM	130
Introduction to the Screen Capture module and AIM	131
Installation in a Citrix or Terminal Services environment	132
Supported Terminal Server sessions	132
Limitations and best practices	133
Citrix published applications	133
Citrix published applications Screen Capture limitations	133
Capture Service and Recorder Integration Service limitations	135
Memory utilization on a Terminal Server	135
Installation on Azure Virtual Desktop	136
Installation in an Amazon WorkSpace environment	137
Screen Capture and AIM registry settings	139
Registry key locations	139
Screen Capture registry values	139
Screen Capture specific entries	149
Filter logon types for Screen Capture Agent	151
Filter rules for Selective Screen Application Recording	152

Selective Screen Application Recording registry example	155
Registry values for Terminal Services support	156
AIM registry values	156
Configuration required to support AIM call annotation	167
Configure AIM to support annotations	168
Configure custom attributes in Enterprise Manager	169
Enable custom data fields and mapping attributes	171
Configure custom data in the adapter	172
Verify the configuration is working	172
Troubleshoot the configuration	173
Enable multi-monitor Screen Capture support	174
Encrypt screen recordings in-transit	176
Use a proxy server for screen capture	177
Screen capture proxy for live monitoring on Chrome configuration	178
Known issues for the Screen Capture module	179
Windows 7 Terminal Server issue	179
Windows 7 and Windows 2008 R2 issues	180
Remote Desktop connection issue	180
Windows Media Player capture issue	180
Bandwidth usage and disk storage space conservation with Screen Capture	181
Upgrades do not change the ColorReduction registry setting	181
Screen stitching within segment not supported	182
Screen Capture module failed to capture screens	182
Screen Capture module failed to capture screen and application data	183
Black screen when playing a large screen file on a dual monitor	183
Black screen in SCN file after disabling monitor	183
Color palette change in Aero mode on Windows 7	183
Agent screen resolution modification during recording is not supported	183
Agent screen size modification is not supported	184
Selective Screen Application Recording: Aero Peek, Alt+Tab, and Win Key+Tab not supported	184
Agent screen display settings change requires system restart	184
CapTestB utility	185
Introducing the CapTestB utility	185
CapTestB security	185
CapTestB system requirements	186
Run the CapTestB utility	186
Control bar	187
Statistics grid	189
Performance analysis	190
Media Encoder	191
Media Encoder overview	192

Convert audio files	193
Enable the convert option	193
Disable the convert option	194
Convert from the command line	194

About this guide

Welcome to the *Desktop Applications Deployment Reference and Installation Guide*. Desktop Applications are client applications installed on user workstations to facilitate users to perform their role within the enterprise.

Intended audience

This guide is designed to be used by:

- Customer IT staff responsible for site preparation and installing workstations.
- Professional services staff responsible for planning and setting up the system.

Document revision history

Revision	Description of changes
1.34	Minor edits.
1.33	In <i>Strategic Planner Configuration</i> , added example URL and proxy configuration.
1.32	In <i>Install Screen Capture and AIM manually</i> , added manual installation instructions for the Integration Services Options page.
1.31	In <i>Install Form Designer manually</i> , added a note stating that the installation of Form Designer requires Administrator privileges. If you do not have these privileges, a pop-up window appears before the Installation Wizard runs, asking you for your Elevated User Details.
1.30	In <i>Add Process Discovery Menu to Microsoft Office Visio</i> , added a note stating that Process Discovery is also supported in Microsoft Office 365.
1.29	In <i>Supported operating systems</i> , added a bullet about Chrome OS.
1.28	In <i>Generate an Internal API Key</i> , added a note to clarify that users must sign in under the desired tenant scope.

Revision	Description of changes
1.27	In <i>Thin Clients and VMware</i> , clarified that Azure Virtual Desktop and VMware Horizon 8 are also supported by DPA, Work Assist, and DMS.
1.26	<ul style="list-style-type: none"> In <i>Browser Settings</i>, added Safari 15 and 14. Updated <i>Installation on Azure Virtual Desktop</i> to indicate that the XDDM display driver is required for Windows 10, but not Windows 11.
1.25	Rebranded Avaya OneCloud CCaaS to Avaya Experience Platform™
1.24	<ul style="list-style-type: none"> Added Important note in <i>Desktop Resources</i> for multi-tenant environments. Removed outdated list of Universal Windows Platform (UWP) applications in the entry for SSAR_Processes in <i>Screen Capture registry values</i>. Added details for V15.2 and V15.1 encryption in <i>Encrypt screen recordings in-transit</i>.
1.23	<ul style="list-style-type: none"> The Standalone Form Designer is now deprecated. Removed references throughout the guide. Removed section <i>Playback behavior with different Player types</i>.
1.22	Clarified the versions of the DPA client that can be installed side by side in <i>DPA client upgrade</i> .
1.21	Updated with 2022R1 tech stack updates, such as Windows Server 2022.
1.20	Changed browser support for Chrome and Safari browsers on MAC OS to MAC OS 12.5.1 Monterey.
1.19	<ul style="list-style-type: none"> Added support for semicolon (;) separators in some Screen Capture parameter descriptions. In <i>Thin clients and VMware</i>: <ul style="list-style-type: none"> Added VMWare Horizon 8 support for Face-to-Face Voice Interaction Recorder. Added <i>Cloud virtual environments</i> subtopic.
1.18	<ul style="list-style-type: none"> In <i>Supported operating systems</i>, added Windows 11 support for Face-to-Face Voice Interaction Recorder and Screen Capture Module. In <i>Thin clients and VMware</i>, added VMWare Horizon 8 support for Screen Capture Module.
1.17	Minor text edits.

Revision	Description of changes
1.16	Added "Supported operating systems" sub-topic in the "Install Screen Capture and AIM manually" topic.
1.15	Added the "Windows 11 installations" subtopic in the "Filter rules for Selective Screen Application Recording" topic.
1.14	<ul style="list-style-type: none"> In "Install Screen Capture and AIM manually", on the "Terminal Services configuration" page, added a sub-step to enter the Integration Service hostname and port number. Removed Work Assist.
1.13	Added Work Assist.
1.12	<ul style="list-style-type: none"> Modified AUTH_TOKEN description in the <i>Desktop Resources silent install parameters</i> topic. Added reference to <i>Cloud Enterprise Manager Configuration and Administration Guide</i>.
1.11	<ul style="list-style-type: none"> In the <i>Browsers</i> topic, added <i>Chrome and Edge considerations</i>.
1.10	<ul style="list-style-type: none"> Added the topic <i>Installation in an Amazon WorkSpace environment</i> in the <i>Screen Capture module and AIM</i> chapter. Added the topic <i>Screen Capture failed to capture screen and application data</i> to the <i>Known Issues for the Screen Capture module</i>. Revised <i>Screen Capture configuration requirements</i> in the <i>Installation on Azure Virtual Desktop</i> topic.
1.09	Added the topic <i>Screen Capture module failed to capture screens</i> to the <i>Known issues for the Screen Capture module</i> .
1.08	<ul style="list-style-type: none"> Added multi-user support for Screen Capture in the "Installation on Azure Virtual Desktop" topic. Changed "Windows Virtual Desktop" to "Azure Virtual Desktop" in the <i>Installation on Azure Virtual Desktop</i> topic.
1.07	<ul style="list-style-type: none"> Added the topic <i>Desktop Applications update policy</i>. In the <i>Thin clients and VMware</i> topic, updated the Citrix Virtual Apps/Desktop version to 1916.

Revision	Description of changes
1.06	2021R1 updates: <ul style="list-style-type: none">• Added support for Chrome on Chromebook.• Added support for Firefox 78.• In the Screen capture proxy for live monitoring on Chrome configuration topic, added a requirement to establish connection to the Secure Web Socket.
1.05	Added the topic <i>Configure the Player to use ActiveX playback when using Internet Explorer in Windows</i> .
1.04	Updated browsers supported for Selective Screen Application Recording and added new registry setting SSAR_SupportedBrowsers.
1.03	Added the topic <i>Installation on Windows Virtual Desktop</i> for screen capture.
1.02	<ul style="list-style-type: none">• In <i>Desktop Messaging silent install parameters</i> topic, updated the valid value of USEFQDN to Y only.• Updated the Strategic Planner installation path.• Removed references to Desktop Gadgets application.
1.01	<ul style="list-style-type: none">• Updated the Microsoft Report Builder requirement for Ad-hoc reporting.• Added Windows Server 2019 support.• Updated the topic <i>Thin clients and VMware</i>.
1.00	New document for cloud.

Getting started

Before you begin installing or upgrading each desktop application, you must understand the installation workflow, and which applications are applicable to each type of user.

Topics

Desktop Applications installation workflow	14
Desktop Applications update policy	15
Desktop Applications matrix	16
Obtain the installation packages	18

Desktop Applications installation workflow

The following workflow describes the steps required for installing or upgrading desktop applications on the end user workstations.

Workflow

1. **Plan:** Which desktop applications require installing? See [Desktop Applications matrix \(page 16\)](#).
2. **Prepare:** Ensure the desktops (end user workstations) meet the minimum specifications. See [Customer requirements \(page 19\)](#).
3. **Install:** Decide on the Installation Method. Desktop applications can be batch installed silently or individual applications can be manually installed as needed.
 - **Batch Install Desktop Applications by Silent Distribution:** Silent distribution is used to batch install multiple desktop applications. Each batch contains installation scripts based on the desktop user role and privileges. Example scripts are provided for Agents, Supervisors and Managers, Administrators and Analysts, based on the user's predefined default privileges. See [Customer requirements \(page 19\)](#) and [Installation by role: silent distribution \(page 36\)](#).
 - **Install Individual Desktop Applications Manually:** Desktop Applications can be installed manually on individual workstations. For thin client environments, manual installation is the only supported installation method. See [Installation by application \(page 46\)](#)
4. **Administer:** System administration of the desktop application is required at times, for example, when the Application Load Balancer address changes need to be reflected in the desktop application configuration registry. See [Advanced administration for desktop applications \(page 116\)](#)
5. **Upgrade:** If upgrading to desktop applications compatible with systems from previous suite versions, follow the upgrade instructions. See [Upgrade legacy desktop applications \(page 124\)](#).

Desktop Applications update policy

Desktop Applications can be updated to the latest version any time, regardless of the update release version installed on the servers or on the cloud.

In addition, the Desktop Applications are compatible with newer update releases for two update releases going forward. Therefore, to keep pace with installed update release, Desktop Applications must be updated to the latest version periodically.

The best practice is to update the relevant Desktop Application to the latest version every time a new update release version becomes available, or at least once a year as a minimum.



On the desktops software download page, sort the table by date and look for the newest clients since your last update. The relevant Desktop Applications are based on your deployment.

Related topics

[Obtain the installation packages \(page 18\)](#)

Desktop Applications matrix

The Desktop Applications Matrix provides a quick reference to the applications and their relevancy for the user.

Product	Desktop Application	Function	Agents	Supervisors and Managers	Admin and Analysts
All products	Desktop Messaging Client (Pop-up Notification)	Sends notices to agents manually, or automatically based on performance parameters.	✓	✓	✓
All products	Desktop Resources	Desktop Resources is a prerequisite package that includes mandatory resources required by all desktop applications .	✓	✓	✓
All products	Logger	Required for viewing log information for troubleshooting purposes. * Agent Logging can also use the log component of the Screen Capture Module.	*	✓	✓
DPA	DPA Client	Captures employee desktop activity data according to defined rules and executes DPA triggers such as stop/start recording, message prompts, and guidance scripts.	✓		

Product	Desktop Application	Function	Agents	Supervisors and Managers	Admin and Analysts
DPA	DPA Process Discovery	Provides a means to discover workflow variations between users and to visualize these workflows as Microsoft Visio diagrams.			✓
QM	Form Designer	Creates and manages evaluation and assessment forms. *A Supervisor or Manager may require the Form Designer if they have Administer privileges.		*	✓
Recording	Face-to-Face Voice Interaction Recorder	Allows employees to record audio and screen activity for in-person interviews from a laptop or desktop computer, while in a location such as a branch office or client site.	✓	✓	
Recording	Screen Capture and AIM	Triggers audio recording, screen capture and provides logging information.	✓		
Recording Speech Analytics QM	Player	Required for playing audio and screen files from the Portal.		✓	✓
WFM	Strategic Planner	Strategic resource planning.		✓	

Obtain the installation packages

Obtain the installation packages from the portal or from your service representative.

For Face to Face Voice Interaction Recording, see the *Face to Face Voice Interaction Recording Installation and Configuration Guide* for instructions.

Customer requirements

The hardware and software required for the Desktop Applications is described.

Topics

Operating systems	20
Thin clients and VMware	22
Hardware specifications	25
Browser Settings	26
Configure workstations in TLS environment	28
Third-party software required by desktop applications	30
Third-party software required for browsing	32
Localization	33
Folder permissions	34

Operating systems

The supported operating systems, security settings, firewalls and antivirus settings are described.

Related topics

[Supported operating systems \(page 20\)](#)

[Windows security settings \(page 20\)](#)

[Windows firewalls \(page 21\)](#)

[Antivirus settings \(page 21\)](#)

Supported operating systems

The supported operating systems for Desktop Applications installed on the end user machine include:

- Microsoft Windows Server 2022 (with Desktop Experience) Standard and Datacenter editions
- Microsoft Windows Server 2019 (with Desktop Experience) Standard and Datacenter editions
- Microsoft Windows Server 2016 (with Desktop Experience) Standard and Datacenter editions
- Microsoft Windows Server 2012 R2 (Server with a GUI) Standard and Datacenter editions
- Microsoft Windows 11 Pro and Enterprise 32-bit and 64-bit
- Microsoft Windows 10 Pro and Enterprise 32-bit and 64-bit
- macOS X 10.10 Yosemite and later is supported only for browsing with Chrome or Safari.
- Chrome OS 87 and later is supported only for browsing with Chrome.



The Phonetics Boosting Desktop application supports only the 64-bit operating system. For a localized OS, install the English Language Pack and set English language as the default.



For the Face-to-Face Voice Interaction Recorder, the supported operating systems are Microsoft Windows 10 and 11 Enterprise/Professional 32-bit and 64-bit.

Windows security settings

Desktops applications support TLS communication only.

For hybrid cloud with site servers of previous versions (V11.1 and V15.1), non-TLS communication is also supported from desktops to the site servers in certain environments (refer to the *Upgrade legacy desktop applications* section).

Related topics

[Configure workstations in TLS environment \(page 28\)](#)

[Upgrade legacy desktop applications \(page 124\)](#)

Elevate UAC security

The Desktop Applications installation files must be run as a Windows Administrator. By default, the Windows 7 and above or Windows 2008 R2 and above User Account Control (UAC) security feature is enabled to control Standard User access. As a result, UAC security elevation is required in order to gain the administrative access required for running the installation files.

Procedure

1. Open a **Command Prompt**, right-click and select **Run as administrator**.
2. If prompted for the user name and password, provide administrator credentials.
3. When the command prompt opens, run the relevant Desktop Application installation file.
4. Continue the installation according to the procedure relevant to the Desktop application you are installing.

Windows firewalls

If any local Windows firewalls or organizational firewalls are enabled on the workstations, it is required to open ports for the Desktop Applications and for browsing to the Portal from the workstations.

Related information

Port requirements (*Avaya Experience Platform™ Workforce Engagement Technology, Security, & Network Integration Deployment Reference Guide*)

Port requirements (*Avaya Experience Platform™ Workforce Engagement Technology, Security, & Network Integration Deployment Reference Guide for Hybrid Cloud*)

Antivirus settings

When real-time antivirus scans are used, there may be file extensions, files and folders that should not be scanned by antivirus applications. To prevent scanning these files, make sure that the exclusion list for each desktop is set up for the applications.

Related information

Desktop antivirus requirements (*Avaya Experience Platform™ Workforce Engagement Technology, Security, & Network Integration Deployment Reference Guide*)

Desktop antivirus requirements (*Avaya Experience Platform™ Workforce Engagement Technology, Security, & Network Integration Deployment Reference Guide for Hybrid Cloud*)

Thin clients and VMware

Desktop Applications can run remotely on CITRIX (HDX technology is supported) or Terminal Server thin client, and VMware environments. In thin client environments, manual installation of the Desktop Applications is the only supported installation method, except for the Screen Capture module, which supports silent installation in all cases.

The hardware specifications for Remote Desktop Services/Terminal Services are proportional to the number of simultaneous users accessing the these services. Take into consideration the user profile and the applications they use.

Thin clients and VMware

Supported thin client and VMware environments for each of the Desktop Applications is listed.

Virtual environments	Comments
Windows 2019 64-bit Edition with: <ul style="list-style-type: none"> • Citrix Virtual Desktop 1912 LTSR for Windows 10 • Citrix Virtual Desktop 2203 LTSR for Windows and 11 (Single and Multi-session) • Citrix Virtual Apps Apps 1912 LTSR for Windows 10 • Citrix Virtual Aps 2203 LTSR for Windows 10 and 11 (Single and Multi-Session) 	Supported by all desktop applications except: <ul style="list-style-type: none"> • Desktop Messaging Client if Published Application • Face-to-Face Voice Interaction Recorder
Windows 2012 R2 64-bit Edition with: <ul style="list-style-type: none"> • Remote Desktop Session Host (RD Session Host) • Citrix Virtual Apps/Desktop 1912 • Citrix 32-bit/64-bit XenApp 7.x** • Citrix 32-bit/64-bit XenDesktop 7.x** 	
Windows 2008 R2 SP1 64-bit Edition with: <ul style="list-style-type: none"> • Remote Desktop Session Host (RD Session Host) • Citrix 32-bit/64-bit XenApp 6.5/7.x** • Citrix 32-bit/64-bit XenDesktop 7.x** 	

Virtual environments	Comments
VMware Horizon 8	<p>VMware Horizon 8 is supported by:</p> <ul style="list-style-type: none"> • Screen Capture Module • Face-to-Face Voice Interaction Recorder • Desktop and Process Analytics • Work Assist • Desktop Messaging Services
Windows 2012 R2 / 2016 / 2019 / 2022 Remote Desktop Services	<p>Supported by all desktop applications except:</p> <ul style="list-style-type: none"> • Face-to-Face Voice Interaction Recorder

Face-to-Face Voice Interaction Recorder limitations for VMware Horizon 8:

- A virtual machine is always assigned to the same user, and more than one user cannot use the same virtual machine.

DPA limitations on Citrix, Terminal Services, and VMware:

- Validator's accessibility feature is not supported.

** The system must be added to the exclusion list of Citrix's Virtual Memory Optimization feature.

Cloud virtual environments

Virtual environments	Comments
<p>Amazon WorkSpaces with:</p> <ul style="list-style-type: none"> • Windows 10 Desktop Experience 	<p>Amazon WorkSpaces is only supported by the Screen Capture Module and the Face-to-Face Voice Interaction Recorder.</p> <div>  Amazon Linux WorkSpaces are not currently supported. </div>
<p>Azure Virtual Desktop with:</p> <ul style="list-style-type: none"> • Windows 10 Enterprise • Windows 11 Enterprise 	<p>Azure Virtual Desktop is supported by:</p> <ul style="list-style-type: none"> • Screen Capture Module and the • Face-to-Face Voice Interaction Recorder. • Desktop and Process Analytics • Work Assist • Desktop Messaging Services

Face-to-Face Voice Interaction Recorder limitations on cloud virtual environments:

- In Azure Virtual Desktop and Amazon Workspaces installations of Face-to-Face Voice Interaction Recorder, a virtual machine is always assigned to the same user, and more than one user cannot use the same virtual machine.

Related topics

[Screen Capture module and AIM \(page 130\)](#)

[Supported Terminal Server sessions \(page 132\)](#)

Hardware specifications

For hardware requirements for the workstations, refer to the *Customer Furnished Equipment (CFE) Guide*.

Browser Settings

The web applications support the specified browsers.

- Google Chrome, v45 or higher on Windows 32 bit and 64 bit.
- Google Chrome, v65 or higher on MAC OS 12.5.1 Monterey.
- Google Chrome on Chromebook 87 or higher.
- Safari 15 and 14
- Firefox for Windows, version 91 ESR or higher.
- Microsoft Edge (current on Chromium engine - v100 or higher).

Chrome and Edge considerations

Due to update schedules of Microsoft and Chrome, DPA can no longer guarantee URL detection in the Chrome and Edge browsers without appropriate browser extensions installed.

Appropriate DPA Chrome extensions can be downloaded from the Chrome store. The URL detection inline is retained with the browser updates.

Chrome OS 87 and later is supported only for browsing with Chrome.

Browser requirements for the Player

Interaction playback in Chrome, Edge, Firefox, or Safari using streaming, does not require installation of the Plugin Player on the client workstation. The Streaming Player uses the native browser capabilities to perform playback.

Related topics

[Player \(page 86\)](#)

General Chrome settings

The general Chrome settings apply to all desktop applications.



The location of the settings is according to Chrome Version 84. It may change according to Chrome updates.

Location

In Chrome, go to **Settings > Advanced Settings > Privacy and security > Site Settings**.

Portal address format

Where required to add the portal address (URL) to the exceptions list, add a wildcard (*) to the URL to allow all portal addresses.

Site Settings

Setting	Requirement	Purpose
Cookies and site data	<ol style="list-style-type: none"> 1. Select <i>Cookies and site data</i>. 2. Add the portal address to the list of sites allowed to use cookies. 	The system uses cookies to maintain user sessions, LB persistence, and so on.
Startup	<ol style="list-style-type: none"> 1. Under <i>Cookies and site data</i>, select <i>Clear cookies and site data when you quit Chrome</i>. <p>Or</p> <ol style="list-style-type: none"> 1. Go to <i>Settings</i>. Under <i>On Startup</i>, clear <i>Continue where you left off</i>. 2. Go to <i>Settings > Advanced Settings</i>. Under <i>System</i>, clear <i>Continue running background applications when Google Chrome is closed</i>. 3. Go to <i>Settings > Advanced Settings</i>. Under <i>Privacy and security</i>, clear <i>Allow Chrome sign-in</i>. 	This ensures user sessions end when the browser is closed. Otherwise, the session may remain open until it times-out (by default after 1 hour). During this time, the user can log in automatically without entering a password.
Images	Under <i>Images</i> , select <i>Show all</i> .	Required to show the images and icons of the Player application.
JavaScript	Under <i>JavaScript</i> , select <i>Allowed</i> , and add the portal address to the list of sites allowed to run JavaScripts.	Required for JavaScript.
Pop-ups	Under <i>Pop-ups</i> , select <i>Allowed</i> , and add the portal address to the list of sites allowed to display pop-ups.	Required for the following pop-up windows: login, Interaction administration applications, play screen in a new window, and DPA portal.
Automatic Downloads	<p>Under <i>Automatic Downloads</i>, do one of the following:</p> <ul style="list-style-type: none"> • Select <i>Ask when a site tries to download files automatically after the first file</i> • If you choose to disable downloads, add the portal address to the list of sites allowed to download automatically. 	Required for downloading files from the portal, such as DPA validator, and reports.

Configure workstations in TLS environment

Configuring TLS in workstations is required in a cloud environment, except for legacy site servers in a hybrid cloud.

In TLS environment, Desktop applications initiate a handshake process with the server. The TLS server then responds with its server certificate. The Desktop Applications must trust the Certificate Authority in order to trust the TLS server certificate. For this purpose, the certificate of the Certificate Authority must be included in the list of Trusted Root Certification Authorities stored on the workstations running desktop applications.

You are required to provide the TLS certificates during initial installation, and as part of on going maintenance (such as certificate expiration or replacement).

Before you begin

Verify you have loaded certificates to the each workstation's certificate store as directed in [Install Root CA certificates on workstations \(page 28\)](#)

Procedure

1. Set browsers to support HTTPS in **Modern** mode (optional).
When the enterprise **HTTPS Protocol and Cipher** configuration is set to **Modern**, enable TLS 1.2 in your browser and workstation settings as well.
2. Update the desktop applications configuration settings.
By default the desktop applications are configured as non-HTTPS, in order to use HTTPS, it is required to update the Desktop Applications configuration settings.

Install Root CA certificates on workstations

Install Root CA certificates on workstations for Windows and Java Trusted Root Certificate Authorities store.

Add Root CA certificates to workstation Windows Trusted root certificate authorities store

Use this procedure for web and desktop applications to trust the CA certificate(s).

Procedure

1. In the **Start** menu, type **mmc** and click **Enter**.
2. In the Microsoft Management Control window, click **File > Add/Remove Snap-in**.
3. Click **Certificates**, click **Add**, select **Computer Account**, and click **Next**.
4. Select **Local Computer**, click **Finish** and then click OK.
5. In the console tree, double-click **Certificates**.
6. Right-click the **Trusted Root Certification Authorities store**.

7. Click **All Tasks >Import** to add the certificates and follow the steps in the Certificate Import Wizard. Load the prepared certificate.
8. Repeat step 7 until all root CA certificates used in the system are imported.

Add workstation root CA certificates to Java Trusted Certificates

Use this procedure for web based desktop applications using JRE to trust the CA certificate(s).

Procedure

1. On all desktop workstations running JRE, open the **Java Control Panel**.
2. Select the **Security** tab and click **Manage Certificates**.
3. In the **Certificate type** list, select **Trusted Certificates**.
4. From the **User** tab, click Import and browse to the CA certificate location.
5. Select the **root CA** certificate and click **Open**.
6. Repeat steps 4 and 5 until all root CA certificates used in the system are imported.
7. Click **Close** and then **OK**.

Related topics

[Third-party software required for browsing \(page 32\)](#)

Related information

Microsoft documentation ([Manage trusted Root Certificates](#))

Third-party software required by desktop applications

The minimum third party software requirements for each Desktop Application installed on the end user machines must be met.

Desktop application	Required third party software
Desktop Resources	<ul style="list-style-type: none"> • Microsoft Windows Installer 5.0 or higher
Desktop Messaging (Pop-up Notification) Also includes: Desktop Connection Manager	<ul style="list-style-type: none"> • Microsoft Windows Installer 5.0 • Microsoft .NET Framework 4.6.2 or later
DPA Client	<ul style="list-style-type: none"> • Microsoft Windows Installer 5.0 • Microsoft .NET Framework 4.6.2 or later • Microsoft Message Queue (MSMQ) <ul style="list-style-type: none"> ■ MSMQ is required for all versions of the DPA Client. The MSMQ Server and MSMQ Server core features are required. (Restart is required before installing the DPA client.) • Microsoft Visual C++ 2015 Redistributable or higher <ul style="list-style-type: none"> ■ On a 64-bit system, both 32-bit and 64-bit redistributable must be installed.
DPA Validator	<ul style="list-style-type: none"> • Microsoft .NET Framework 4.6.2 and higher versions supported by Microsoft on the Windows operating system • Microsoft Visual C++ 2015 Redistributable or higher (both 32-bit and 64-bit redistributable)
Face to Face Interaction Recorder	<ul style="list-style-type: none"> • .NET Framework version 4.6.1 or later • Microsoft Visual C++ 2015 Runtime Redistributable Package (x86)
Form Designer	<ul style="list-style-type: none"> • Microsoft Windows Installer 5.0 or later

Desktop application	Required third party software
Logger	<ul style="list-style-type: none"> • Microsoft Windows Installer 5.0 or later • Microsoft .NET Framework 4.6.2 or 4.7.x, or 4.8.x • Microsoft Visual C++ 2015 Redistributable 32-bit or later SP/update
Plugin Player	Chrome, Edge, and Safari requirements: None
Screen Capture Module (including AIM)	<ul style="list-style-type: none"> • Microsoft Windows Installer 2.0 or later • Microsoft .NET Framework 4.6.2 or later • Microsoft Visual C++ 2019 Redistributable 32-bit <p>Microsoft Visual C++ 2019 Redistributable 64-bit or later SP/update is required if Selective Screen Application Recording is used on a 64-bit operating system</p>
Strategic Planner	<ul style="list-style-type: none"> • Microsoft Windows Installer 5.0 or later • Java Run-time Environment (JRE) 8.0 (32-bit), including all approved minor version releases • Visual C++ Redistributable for Visual Studio 2012 Update 4 <div>  Verify that the JAVA_HOME environment variable is set to the 32-bit installation of Java. </div>
Ad-hoc reporting	<ul style="list-style-type: none"> • Microsoft Report Builder (latest version)

Third-party software required for browsing

To enable user workstations to browse to the web-based applications, the prerequisite software must be installed.

Software	Web based applications
Acrobat Reader Version: 11 and higher	Required for printing reports
Windows Media Player 12	<ul style="list-style-type: none"> Required to listen to sound prompts and customer recordings in Customer Feedback Required to play back files using Windows Media Player from workstations, without browsing to the Interactions Home Page
Any media player capable of playing back two streams of H264 video (for example, VLC media player)	Required for playing back both sides of a video interaction

SQL Server Report Builder installation requirements

When installing the Report Builder, do not change its defaults. Also, leave blank the Default Target Server setting. If Report Builder was previously installed and a default target server was added during installation, remove or change that element from the configuration file.

- **File:** C:\Program Files (x86)\Microsoft SQL Server\Report Builder\MSReportBuilder.exe.config,
- **Element:** <setting name="DefaultReportServer" serializeAs="String">

Set the target server URL for the reports in the Ad Hoc Reports page in the system portal.

In addition, to force TLS security, verify that the following registry key is added:

- For 64-bit OS:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\v4.0.30319
"SchUseStrongCrypto"=dword:00000001
- For 32-bit OS:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NETFramework\v4.0.30319
"SchUseStrongCrypto"=dword:00000001

Localization

The Desktop Applications support localized systems. The localization includes the user interface and the On-Line Help (OLH). Desktop Applications support localization of more than one language simultaneously.

For details about the supported languages, contact your service representative.

Folder permissions

Folders used by the desktop applications, require specified permissions after installation and at a run-time.

Desktop application	Folders	Permissions after installation	Permissions required at a Run-time
Screen Capture (requires KB150400)	%PROGRAMFILES%\VERINT\CaptureService	Read / execute for authenticated user	Read / execute for Authenticated user
Screen Capture (requires KB150400)	%PROGRAMFILES%\VERINT\CaptureService\Screen Capture Module\Logs	Authenticated users with full control	Read / execute / write for authenticated user
DPA Client	%PROGRAMFILES%\VERINT\DPA\Client	Inherited from parent	Read / execute for all users
DPA Client	%PROGRAMDATA%\VERINT\DPA\Data	Inherited from parent	Read / write / delete for all users
Desktop Messaging	%PROGRAMFILES%\VERINT\DPA\Client	Inherited from parent	Read / execute for all users
Desktop Messaging	%PROGRAMDATA%\VERINT\DPA\Data	Inherited from parent	Read / write / delete for all users
Desktop Resources	%PROGRAMDATA%\VERINT\DesktopResources	Inherited from parent	Read / execute for all users
Player	%PROGRAMFILES%\Verint\Playback	Inherited from parent	Read / execute for all users
Form Designer	%PROGRAMFILES%\Verint\FormDesigner	Inherited from parent	Read / execute for all users
Strategic Planner	%PROGRAMFILES%\Verint\StrategicPlanner	Inherited from parent	Read / execute for all users
Logger	%PROGRAMFILES%\Verint\Logger	Inherited from parent	Read / execute for all users



Related to all desktop applications: "List Folder Contents" permissions for folder.

Installation by role: silent distribution

Silent distribution is used to batch install multiple desktop applications on the end user workstations. Each batch contains the installation scripts for the desktop applications required, based on the user role and their associated privileges.

Topics

Silent distribution guidelines 37

Silent distribution for agents 39

Silent distribution for supervisors/managers41

Silent distribution for administrators and analysts43

Silent distribution guidelines

Silent distribution is used to batch install multiple desktop applications on the end user workstations. Each batch contains the installation scripts for the desktop applications required, based on the user role and their associated privileges.

Desktop applications can be silently installed by any standard distribution and packaging method.

Related topics

[Before you begin a silent distribution \(page 37\)](#)

[Silent distribution workflow \(page 37\)](#)

Before you begin a silent distribution

Before you begin silently distributing the application(s), define a shared folder for the installation scripts, define the installation destinations, and define a group policy.

Procedure

1. Define a Shared Folder to Save the Installation Files:

The installation scripts are saved here. Ensure the workstations can access this location.

- a. Right-click the defined folder and select the **Properties > Sharing** tab:
 - Select **Share this folder**.
 - Click **Permissions**.
 - Grant the Domain Computers group **Read** rights.
- b. Click the **Security** tab, and grant the Domain Computers group **Read, Read and Execute**, and **List Folder Contents** rights.
- c. **Define Organizational Units in the Domain:** Segment the workstations according to the predefined user roles. That is, Agent, Supervisor, Manager, Administrator, and Enterprise Administrator.

2. Define the Installation Destination:

Define the location on the workstations to install the Desktop Applications.

3. Define a Group Policy:

The installation can then be assigned to the relevant group of workstations, and the application(s) are automatically installed next time these workstations are rebooted.

Silent distribution workflow

The system supports the distribution of packages over the network from a central location to the workstations using any standard software distribution tool. The distribution tool automatically installs the applications without requiring user intervention.

Workflow

1. All site preparation and system requirements must be met for each desktop application.
2. Run the distribution script(s) using a standard silent distribution method.
 - If the script contains an installation package of an application already on the workstation, the installation recognizes this and does not reinstall the application.
 - Mandatory parameters must be included and cannot be changed.
 - Silent install parameters are case sensitive and are required to be capitalized.
 - This does not repair faulty installations.
3. On completion:
EXIT_CODE = 0 indicates installation success
EXIT_CODE = 1 indicates installation failure and the workstation reboots silently.
4. The next time the workstations in the defined organizational unit are restarted, the application(s) are installed.

Silent distribution for agents

Agents require Desktop Applications that facilitate audio and screen recording, and logging for troubleshooting purposes.

Related topics

[Desktop Applications for agents \(page 39\)](#)

[Example script for agents \(page 39\)](#)

Desktop Applications for agents

Specified Desktop Applications are required for users defined as Agents.

Agent Desktop applications

- Desktop Resources
- Screen Capture and AIM
- DPA Client
- Desktop Messaging Client

Additional Desktop applications for Portal

The predefined Agent role does not have access to the Portal. If agents are granted access, then add these applications to the script.

- Plugin Player (only required if using IE)
- Logger

Example script for agents

An example script for silently installing the desktop applications for the predefined agent role is provided. Modify the silent parameter default values as required for your specific deployment.

Example script

```
@echo off
setlocal
REM The script uses parameters for silent reboot when reboot is required
REM Continue running the script after each reboot until each script is installed
successfully
REM If installation fails, the EXIT_CODE is 1
set MSIS_DIR=\\<Shared network folder:>\DesktopApplications
set INSTALLFOLDER<component_name>=C:\Program Files\<Company Name>\<component_name>
SET EXIT_CODE=0
echo Desktop Resources Installation
msiexec -i "%MSIS_DIR%\DesktopResourcesAvaya.msi" USE_COMMAND_LINE=1
TARGETDIR="%INSTALLFOLDER%" /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
```

```

echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo Logger Installation
msiexec -i "%MSIS_DIR%\LoggerInstallation.msi" USE_COMMAND_LINE=1
INSTALLFOLDER="%INSTALLFOLDER%" /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo Screen Capture Module
msiexec -i "%MSIS_DIR%\Screen_Capture_Module.msi" USE_COMMAND_LINE=1
INSTALLDIR="%INSTALLFOLDER%\Screen Capture Module" AGENT_MONITORING_ENABLED=TRUE /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo EXIT_CODE is %EXIT_CODE%
exit /B %EXIT_CODE%
echo DPA Client
msiexec /i <PCMonClient.msi or PCMONClient64.msi> CONFIGSERVER=<LBName> USEIEBHO=Y
AUTOSTART=N /q /n
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo Desktop Connection Manager
msiexec /i DesktopConnectionManager.msi SERVERADDR=testing DRSERVER=MyDRServ /q /n
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo Desktop Messaging Client
msiexec /i DMSClientInstall.msi Messaging AUTOSTART=Y
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)

```

Related topics

[Desktop Applications for agents \(page 39\)](#)

Silent distribution for supervisors/managers

Supervisor Workstations require Desktop Applications that facilitate audio and screen playback, agent monitoring, evaluation and assessment, and workforce optimization. Manager Workstations require Desktop Applications that facilitate access and use of all Portal applications.

Related topics

[Desktop applications for supervisors/managers \(page 41\)](#)

[Example script for supervisor/manager \(page 41\)](#)

Desktop applications for supervisors/managers

The Desktop Applications required for users defined as Supervisors and Managers are listed. Links to each application's silent install parameters is also provided.

Supervisors and manager Desktop applications

- Desktop Resources
- Plugin Player (only required if using IE)
- Form Designer
- Desktop Messaging Client
- Strategic Planner
- Logger

Additional Desktop applications

- Screen Capture

The predefined Supervisor and Manager roles are not recorded by default. For workstations that are required to be recorded, install Screen Capture.

Example script for supervisor/manager

An example script for silently installing the desktop applications for the predefined Supervisor or Manager role is provided. Modify the silent parameter default values as required for your specific deployment.

Example script

```
@echo off
setlocal
REM The script uses parameters for silent reboot when reboot is required
REM Continue running the script after each reboot until each script is installed
successfully
REM If installation fails, the EXIT_CODE is 1
set MSIS_DIR=\\<Shared network folder:>\DesktopApplications
set INSTALLFOLDER<component_name>=C:\Program Files\<Company Name>\<component_name>
SET EXIT_CODE=0
echo Desktop Resources Installation
```

```
msiexec -i "%MSIS_DIR%\DesktopResourcesAvaya.msi" USE_COMMAND_LINE=1
TARGETDIR="%INSTALLFOLDER%" /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo Logger Installation
msiexec -i "%MSIS_DIR%\LoggerInstallation.msi" USE_COMMAND_LINE=1
INSTALLFOLDER="%INSTALLFOLDER%" /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo Playback Installation
msiexec -i "%MSIS_DIR%\PlaybackInstallation.msi" USE_COMMAND_LINE=1
INSTALLFOLDER="%INSTALLFOLDER%" ADDLOCAL=Playback IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo Strategic Planner Installation
msiexec /i "%MSIS_DIR%\StrategicPlannerSetup.msi" INSTALLDIR="%INSTALLFOLDER%"
SZAPPSEVERNAME="application_LB_address" SZAPPSEVERPORT="application_LB_port" /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo EXIT_CODE is %EXIT_CODE%
exit /B %EXIT_CODE%
```

Related topics

[Desktop applications for supervisors/managers \(page 41\)](#)

Silent distribution for administrators and analysts

Administrator Workstations require Desktop Applications that facilitate system application administrative functions, and playback of audio and screen files.

Related topics

[Desktop applications for administrators and analysts \(page 43\)](#)

[Example script for administrators and analysts \(page 43\)](#)

Desktop applications for administrators and analysts

The Desktop Applications required for users defined as Administrators are provided.

Administrator Desktop Applications

- Desktop Resources
- Plugin Player (only required if using IE)
- Form Designer
- Desktop Messaging Client
- DPA Process Discovery
- Logger

Example script for administrators and analysts

An example script for silently installing the desktop applications for the predefined agent role is provided. Modify the silent parameter default values as required for your specific deployment.

This example script contains the desktop applications listed in [Desktop applications for administrators and analysts \(page 43\)](#).

Example script

```
@echo off
setlocal
REM The script uses parameters for silent reboot when reboot is required
REM Continue running the script after each reboot until each script is installed
successfully
REM If installation fails, the EXIT_CODE is 1
set MSIS_DIR=\\<Shared network folder:>\DesktopApplications
set INSTALLFOLDER<component_name>=C:\Program Files\<Company Name>\<component_name>
SET EXIT_CODE=0
echo Desktop Resources Installation
msiexec -i "%MSIS_DIR%\DesktopResourcesAvaya.msi" USE_COMMAND_LINE=1
TARGETDIR="%INSTALLFOLDER%" /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
```

```
)
echo Logger Installation
msiexec -i "%MSIS_DIR%\LoggerInstallation.msi" USE_COMMAND_LINE=1
INSTALLFOLDER="%INSTALLFOLDER%" /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo Form Designer Installation
msiexec -i "%MSIS_DIR%\FormDesignerInstallation.msi" USE_COMMAND_LINE=1
VERINTFOLDER="%INSTALLFOLDER%" GLOBAL_APP_SERVER_DNS=LBName GLOBAL_USE_SSL=1 GLOBAL_APP_
SERVER_AUTH_PORT=<443> GLOBAL_APP_SERVER_IIS_PORT=<443>/qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo Playback Installation
msiexec -i "%MSIS_DIR%\PlaybackInstallation.msi" USE_COMMAND_LINE=1
INSTALLFOLDER="%INSTALLFOLDER%" ADDLOCAL=Playback IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo User Import Package Installation
msiexec -i "%MSIS_DIR%\UserImportPackageInstallation.msi" USE_COMMAND_LINE=1
VERINTFOLDER="%INSTALLFOLDER%" /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo DPA Process Discovery
msiexec /i \\VerintServer1\public$\clientMSI\ ProcessDiscoverySetup.msi
INSTALLDIR=%PROGRAM_FILES%\Verint\Process Discovery USEHTTPS=Y PDSEVER=<Application
Load Balancer> WEBSERVICEURL= http://<Application Load Balancer address>
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
) ELSE (
echo ---installer succeeded
)
echo EXIT_CODE is %EXIT_CODE%
```

```
exit /B %EXIT_CODE%
```

Related topics[Desktop applications for administrators and analysts \(page 43\)](#)

Installation by application

The installation steps for each Desktop Application is described.

Topics

Desktop Resources	47
Desktop Supportability	50
Desktop Messaging	51
Desktop and Process Analytics (DPA) clients	57
DPA Process Discovery	78
Form Designer	81
Logger	84
Player	86
Phonetics Boosting	97
Screen Capture and AIM	99
Strategic Planner Client	112
Face to Face Voice Interaction Recording	115

Desktop Resources

Desktop Resources is a pre-requisite package that includes mandatory resources required by all desktop applications.



For any multi-tenant environment: To provide proper authentication and scoping of the desktop connection with the recording system, it is recommended to [Generate an Internal API Key \(page 48\)](#).

Related topics

For all software and hardware specifications refer to [Customer requirements \(page 19\)](#).

Install Desktop Resources manually

The Desktop Resources manual installation procedure must be performed on the desktop on which the dependent desktop applications will run.



When uninstalling the desktop applications, Desktop Resources must be uninstalled last, after all other desktop applications are uninstalled.

Before you begin

- Download the Desktop Resources installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. To launch the Setup Wizard, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.
 - OR
 - If installing from the media, double-click the **DekstopResources<company>.msi**.
2. When prompted for an Authentication Token, enter the internal API key (see Related topics, below).
3. If a security warning appears, click **Run** and continue the installation.
The installer asks you to wait while it configures the Desktop Resources, and closes automatically.

Related topics

[Generate an Internal API Key \(page 48\)](#)

Desktop Resources silent install parameters

The property settings determine how Desktop Resources is installed silently on the desktops.

Updating existing property settings

To change property settings after installation, you can reinstall the Desktop Resources MSI with new silent installation parameters.

Reinstalling with new parameters does not require uninstalling the existing desktop resources.

Parameters	Description and Default Values
AUTH_TOKEN	The internal API key value used for tenant authorization. Used for authentication in Capture Service and related components. If coding custom integrations with the Verint software, an AUTH_TOKEN needs to be obtained using the License Manager. Default value: (empty) Mandatory
MSIS_DIR	<Shared network folder:>\DesktopApplications
MsiFile	DesktopResourcesAvaya.msi
USE_COMMAND_LINE	USE_COMMAND_LINE=1 Mandatory

Related topics

Refer to [Installation by role: silent distribution \(page 36\)](#) for a sample script that includes the command line for distributing this application in silent mode.

[Generate an Internal API Key \(page 48\)](#)

Related information

Authentication flow (*Workforce Optimization SDK Programmer's Guide*)

API keys (*Cloud Enterprise Manager Configuration and Administration Guide*)

Generate an Internal API Key

To include the AUTH_TOKEN parameter in the Desktop Resources installation, you must provide an internal API key. You can generate the key through License Management.

Before you begin

You must have appropriate access rights to generate the key and show the key value.

Procedure

1. Sign in as the tenant administrator.



You must sign in under the desired tenant scope for the target desktops. Logging in under the service provider scope will generate an API key for the service provider scope, and not the tenant scope.

2. Go to **System Management**. Under **License Management**, select **API Keys**.
3. Select the Add icon .
4. Set the **Key Type** to Internal.
5. Optional: Add a description for the key, such as *Desktop Resources API key*.
6. Select **Generate**.
7. Under **Actions**, select the Show  icon.
8. Under **Actions**, select the Copy  icon.
9. Use the copied value as the value for the Desktop Resources AUTH_TOKEN parameter.

Related topics

[Desktop Resources silent install parameters \(page 48\)](#)

Desktop Supportability

The Desktop Supportability feature enables a desktop host to register with the data center. It can then provide information about the installation, as well as current status information. It also supports requests to upload log files directly to the application server.

Install Desktop Supportability

To use the Desktop Supportability feature, you must install both of the following:

- Desktop Resources, with an appropriate internal API key
- Desktop Messaging, with the Desktop Connection Manager

Related topics

[Desktop Resources \(page 47\)](#)

[Desktop Messaging \(page 51\)](#)

Desktop Messaging

Desktop Messaging is a scalable, real-time message delivery system that includes capabilities from analytics engines such as voice biometrics.

An administrator, manager, supervisor, or scheduler can send desktop (pop-up) messages to employees by using their name, login or role within their organization. Alternatively, administrators can configure automatic messaging based on conditions such as out of range KPIs or adherence issues.

Install multiple 15.2 Desktop Messaging clients side by side

New revisions of the 15.2 clients (released with feature packs or following hot fixes) can be installed side by side. All add remove program entries of the installers have a version number (first three digits), and revision numbers.

Desktop Messaging rollback

To revert to a previous 15.2 client version, use the installer to repair back to that version. If you do this without removing the later versions of the client then it is not clear in add remove programs that you rolled back to the earlier version, as the installer revision number will remain as the later version. Best practice is to un-install the later version and then repair the client wanted for rollback.

Workflow: Install Desktop Messaging manually

Desktop Messaging requires installing a shared connection manager that configures the desktop with the Application Load Balancer.

Workflow

1. Meet all customer site preparation requirements for desktop messaging.
2. Install Desktop Resources.
3. [Install Desktop Connection Manager manually \(page 51\)](#).
4. [Install Desktop Messaging manually \(page 53\)](#).

Install Desktop Connection Manager manually

The connection manager stores connection details of the Application Load Balancer. The connection details are shared and used by the Desktop Messaging client.

Manual and silent installation are supported.

Required network capabilities

The DMS Connection service requires network capabilities for full connectivity with the application services. The account used to access the network must have the **Enable the Logon as a Service** right. The default account, NT AUTHORITY\NETWORK SERVICE, typically already has this access right.

Before you begin

- Meet all desktop messaging [Customer requirements \(page 19\)](#).
- Install [Desktop Resources \(page 47\)](#).
- Download the Desktop Connection Manager installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. To launch the Setup Wizard, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.OR
 - If installing from the desktop media, run **DesktopConnectionManager.msi**.
2. In the Welcome screen, click **Next**.
3. Accept the terms in the license agreement, and click **Next**.
4. In the **Destination Folder** screen, click **Next** to accept the default location, or click **Change...** to define a different location, and then click **Next**.
5. Enter the **Server Name** of the Application Load Balancer.
6. Select **Use HTTPS**.
7. Select or clear **Use Fully Qualified User Name**.
 - Select to send desktop messages to employees based on their fully qualified user principal name (UPN) as configured in their contact details.
 - Clear to send desktop messages to employers based on their short Windows login name.
8. Set the **Account Initiating DMS Connection Service**:
 - **Account Name:** The user credential specified to initiate communication from the desktop to the application services. This user is used to run the DMS Connection windows service. Default: NT AUTHORITY\NETWORK SERVICE
 - **Password:** No password is required for the predefined Windows Network Service Account. If the service is configured to use a different account, then the password is required at installation. Default: None (empty)
9. In the **Ready to Install** window, click **Install**.
10. When the installation is complete, the **Completed Setup** window appears.
11. Click **Finish** to exit the installation wizard.
The Desktop Connection Manager runs automatically.

Install Desktop Messaging manually

Perform the installation procedure on the desktop where the application will run.

Before you begin

- [Install Desktop Connection Manager manually \(page 51\)](#)
- Download the Desktop Messaging installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. To launch the Installation Wizard, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.
 - OR
 - ng from the desktop media, double-click **DMSClientInstall.msi**.
2. On the **Welcome** page, click **Next**.
3. On the **End-User License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
4. On the **Destination Folder** page, click **Next** to install to the default folder, or click **Change** to install to a different folder.
5. On the **Ready to Install** page, click **Install**.
6. When the installation is complete, the **InstallShield Wizard Completed** page appears. Click **Finish**.
7. To run Desktop Messaging:
 - **Log off** and log in again to activate the client, or
 - Run **Verint.DMS.DesktopMessagingClient.exe** manually from the destination folder.

What to do next

Following system installation:

- Configure a Desktop Message from the Portal.
- Configure a DPA Organizational Alert to call a Desktop Message on action.

Install Desktop Messaging by silent distribution

Silent distribution is used to batch install the connection manager and desktop messaging clients on the end user workstations.

The client can be silently installed by distributing to workstations without user or IT staff intervention for automatic installation, usually upon login to the workstation. All standard distribution and packaging methods are supported.

Before you begin

Meet all hardware and software specifications.

Procedure

1. Log on to the workstation with administrative rights. If required, add the Install As security option to the Windows registry.
2. Run the script to install
 - desktop resources
 - desktop connection manager
 - desktop messaging

Example:

```
msiexec /i DesktopResourcesVerint.msi USE_COMMAND_LINE=1 AUTH_TOKEN=6D27DA1FDC9BD2A5B1A29C5F8F88653FFC60CCE9204B33338B2382D3B5A0367702C0F2919D24272AEC5526D5FFDC2A28C5678BC667D4712B75B284455FAC23CD /q /n
msiexec /i DesktopConnectionManager.msi SERVERADDR=testing DRSERVER=MyDRServ /q /n
msiexec /i DMSCClientInstall.msi CONFIGSERVER=testing /q /n
```

Related topics

[Desktop Messaging silent install parameters \(page 54\)](#)

Desktop Messaging silent install parameters

The properties determine how all Desktop Messaging clients are configured silently.

Desktop Connection Manager script parameters

Parameters	Description and Default Value
MsiFile	Installation file name: DesktopConnectionManager.msi
SERVERADDR	Application Load Balancer address. Mandatory.
INSTALLDIR	Installation destination path. Default =%Program Files%\<Company Name>\<Application Name>
USEHTTPS	Communication security type. Valid values: Y
USEFQDN	Use fully qualified user principal name (UPN) to send desktop messages. Valid values: Y

Desktop Messaging install script parameters

Parameters	Description and Default Value
MsiFile	Installation file name: DMSClientInstall.msi
INSTALLDIR	Installation destination path. Default =%Program Files%<Company Name> \DesktopMessaging\DMSClient
AUTOSTART	<p>Desktop Messaging client automatically starts when a user logs on to the desktop.</p> <p>AUTOSTART=N: does not start automatically</p> <p>AUTOSTART=Y (default): starts automatically</p> <p>If any other value is specified for the AUTOSTART parameter, or if the AUTOSTART parameter is not included in the command line, then the following key is added to the Windows registry:</p> <ul style="list-style-type: none"> • Location: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run • Key: DMSClient • Value: "C:\%Program Files%\<company_name>\Desktop Messaging\DMSClient\Verint.DMS.DesktopMessagingClient.exe" <p>Example:</p> <pre>msiexec /i \\Server\public\$\clientMSI\Verint.DMS.DesktopMessagingClient.ms i INSTALLDIR=C:\<company_name>\Desktop Messaging\ AUTOSTART=Y</pre>

Uninstall Desktop Messaging manually

Uninstall the desktop messaging client and the connection manager manually, or using a script.

Procedure

1. From **Start > Settings > Control Panel**, open **Add or Remove Programs**.
2. Select **Desktop Connection Manager** and click **Remove**.
3. Select **DMS Desktop Messaging** and click **Remove**.

Uninstall Desktop Messaging silently

Uninstall the desktop messaging client and the connection manager manually, or using a script.

Procedure

1. To uninstall the client, run these scripts:

```
msiexec /x DMSCClientInstall.msi /q /n
```

```
msiexec /x DesktopConnectionManager.msi /q /n
```

2. To uninstall when you do not have the original installer, run this script for the connection manager and the desktop messaging clients:

```
msiexec /x {productcodegoeshere} /q /n /norestart
```

3. To rollback/repair, run these scripts:

```
msiexec /fmasu DesktopConnectionManager.msi/q /n /norestart
```

```
msiexec /fmasu DMSCClientInstall.msi /q /n /norestart
```

4. To rollback/repair when you do not have the original installer, run this script for the connection manager and the desktop messaging clients:

```
msiexec /fmasu {productcodegoeshere} /q /n /norestart
```

Product code

The product code is taken from the pcmonclient.html file of the previous installer or from the registry of a target workstation with the client installed. It is the same for all MSI versions. The brackets {} around the product code are required.

Desktop and Process Analytics (DPA) clients

The DPA client captures employee desktop activity according to defined rules, and executes DPA triggers such as stop/start recording, message prompts, and guidance scripts.

DPA Validator

The DPA Validator utility captures screens, validates screen controls, and displays the screen inside the utility for the user to browse and select controls to be used when defining trigger events. Install DPA Validator. The DPA Validator interface supports all licensed languages.

DPA Process Discovery

The DPA Process Discovery client is a separate installation that adds a Visio based reporting tool for DPA Analysts.

Related topics

[Install the DPA client manually \(page 57\)](#)

[Configure DPA Data Transfer service user name and password \(page 59\)](#)

[Install DPA client by silent distribution \(page 60\)](#)

[Enable DPA to trigger events on web browsers \(page 68\)](#)

[DPA public-private token authentication \(page 71\)](#)

[Uninstall/rollback DPA clients \(page 74\)](#)

[Install DPA Validator \(page 76\)](#)

[Install Process Discovery \(page 78\)](#)

Install the DPA client manually

The DPA client MSI can be used to install, upgrade, or remove Desktop and Process Analytics clients. The MSI conforms to standard Microsoft MSI deployment commands.

Before you begin

- Meet all hardware and software specifications.
- Download the latest DPA client installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. Log on to the workstation with administrative rights.
You must **elevate the UAC security** to gain Windows administrative rights.

- a. From the **Start** menu, select **Programs > Accessories > Command Prompt**.
 - b. Right-click the **Command Prompt** and select **Run as administrator**.
 - c. If prompted for the user name and password, provide administrator credentials.
2. To install the DPA client, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.
 - OR
 - If installing from the media, go to to **<DPA setup files location>\SetupDir\Client_MSI_Install**. Run the PCMONClient.msi (for 32-bit OS) or run PCMONClient64.msi (for 64-bit OS).
3. On the **Welcome** page, click **Next**.
4. On the **End-User License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
5. On the **Destination Folder** page, click **Next** to install to the default folder, or click **Change** to install to a different folder.
Default destination folder: <SoftwareDrive>\Program Files\<Company>\DPA\Client\
6. Set the application **Data Folder**, and click **Next**.
Default data folder: <DataDrive>\ProgramData\<Company>\DPA\Data\
7. Set the **Configuration Information**, and click **Next**.
8. On the **Ready to Install** page, click **Install**.
9. When the installation is complete, the **InstallShield Wizard Completed** page appears. Click **Finish**.

Related topics

[DPA client configuration information \(page 58\)](#)

DPA client configuration information

Use the DPA client installer configuration information table as a guide when configuring the DPA client installation.

DPA client installer configuration parameters

Parameter	Description
Configuration Information	
Server Name	Application Load Balancer address.
Account Initiating DPA File Data Transfer	

Parameter	Description
Account Name	Account name for the DPA file data transfer service that requires network capabilities for full connectivity with the application services. Enable the Logon as a Service right to this account. Default=NT AUTHORITY\NETWORK SERVICE (predefined Windows Network Service Account)
Password	Password for the account name used for the DPA file data transfer service. Default=No The predefined Windows Network Service Account does not require a password.
HTTP/HTTPS	
Use HTTPS	Communication protocol for Avaya Experience Platform™ Workforce Engagement.
Client Auto-Start	
Add Client Auto-Start Registry	Start automatically the DPA client when a user logs on to the desktop.
Additional Options	
Install IE BHO plugin	Required for: <ul style="list-style-type: none">• 64-bit DPA clients installed on Citrix or Terminal Servers.• Deployments using the partial ID match expression feature when validating screens.

Configure DPA Data Transfer service user name and password

Defining a user name and password for the DPA Data Transfer service is an optional procedure. When the DPA client is installed, by default the DPA Data Transfer service is password protected by the settings used on the local workstation's Windows Network Service. When a user name and password is defined for the service, this configuration takes precedence over the Windows Network Service settings, which provides added security for the service on the local client.

Procedure

1. Log on to the workstation with administrative rights.
2. Open a Windows Terminal.

3. Run the following command:

```
msiexec /i pcmonclient64.msi CONFIGSERVER="<your Application Load Balancer address>" SERVICEUSER="<your user name>" SERVICEPWD="<your password>" /qn /passive
```

Install DPA client by silent distribution

Silent distribution is used to batch install DPA clients on the end user workstations. The client can be silently installed by distributing to workstations without user or IT staff intervention for automatic installation, usually upon login to the workstation. All standard distribution and packaging methods are supported.

The DPA silent distribution script can be used to install, upgrade, or remove DPA clients.

Before you begin

Meet all hardware and software specifications.

Procedure

1. Log on to the workstation with administrative rights. If required, add the **Install As** security option to the Windows registry.
2. Run the following script:

```
msiexec /i [path to msi]\[msi file name] INSTALLDIR=path USEIEBHO=Y CONFIGSERVER=servername /q /n
```

Related topics

[Add 'Install As' option \(page 60\)](#)

[DPA client silent distribution script examples \(page 61\)](#)

[DPA client silent script distribution parameters \(page 61\)](#)

Add 'Install As' option

For desktops, to gain Windows administrative rights, add the **Install As** functionality to the Windows registry.

Example: Add 'Install As' functionality

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\Msi.Package\shell\runas]

@="Install &as"

[HKEY_CLASSES_ROOT\Msi.Package\shell\runas\command]

@="msiexec /i \"%1\""

DPA client silent distribution script examples

Examples of DPA client silent distribution scripts with and without optional parameters are provided.

Example: DPA client silent script

This example contains all mandatory parameters.

```
msiexec /i PCMONClient.msi USEIEBHO=Y CONFIGSERVER=<LB> /q /n
```

Example: DPA client silent script with optional parameters

This example contains all mandatory and optional parameters, including data folder, TLS enabled, and auto start.

```
msiexec /i PCMONClient.msi INSTALLDIR=%PROGRAM FILES%\<company_name>\DPA\client  
DATADIR=<DATADIR>\<company_name>\DPA\data USEHTTPS=Y AUTOSTART=Y
```

DPA client silent script distribution parameters

The silent distribution script parameters table provides a description of each switch.

DPA client silent distribution script parameters

Parameter / Switch	Description
/i	Use the msiexec to perform an installation.
[path to msi]	MSI setup file location.
[msi file name]	For 32 bit operating systems, use PCMONClient.msi For 64 bit operating systems, use PCMONClient64.msi
INSTALLDIR	Installation destination path. Default=%Program Files%\<Company Name>\DPA\Client\
USEIEBHO	Installs an IE Browser Helper Object (BHO) plugin. The plugin is required for: <ul style="list-style-type: none"> • All 64-bit clients in Citrix Server and Terminal Services environments. • Deployments using partial web page ID expressions to capture screen controls. Default = N If not included in the script, the default value is assumed.
CONFIGSERVER	Application Load Balancer address.

Parameter / Switch	Description
/q /n	Use the msixexec in unattended mode (this prevents the MSI from prompting for input). Note: You can remove the switches for testing purposes.
DATADIR	Data folder full path to be created by the installer. Default=<DataDrive>\ProgramData\<company>\DPA\Data\
WIX_ACCOUNT_NETWORKSERVICE	Account name for the DPA file data transfer service to connect with the application services. Enable the Logon as a Service right to this account. Default=NT AUTHORITY\NETWORK SERVICE
SERVICEPW	Windows Network Service Account. If specifying a different account, add the password to the script. Default=No password is required for the predefined account
USEHTTPS	Communication protocol. <ul style="list-style-type: none"> • USEHTTPS=Y for Avaya Experience Platform™ Workforce Engagement.
AUTOSTART	Start automatically the DPA client when a user logs on to the desktop. <ul style="list-style-type: none"> • AUTOSTART=Y for automatic start on logon (default) • AUTOSTART=N to prevent automatic start on logon <p>If AUTOSTART=Y, or the parameter is not included in the script, the following key is added to the Windows registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Verint_DCUApp" with a value of "C:\Program Files\Avaya\DPA\Client\mspvdx.exe"</p>

DPA installation in third-party environments

DPA can be installed and report on a number of third-party operating system environments. This section indicates specific steps to ensure reporting where windows operating systems are deployed through virtual or remote methods.

If the third-party environment is controlled or accessed from another workstation that also contains a DPA client, then the data from the remote workstation is reported as the data from the local workstation. This method is available in environments that support Virtual Channels.

In environments that do not support Virtual channels, the remote and local sessions report as two independent data streams coming from separate computers and users.

Related topics

[Install the DPA client for citrix and terminal servers \(page 63\)](#)

- [Citrix published applications \(page 133\)](#)
- [DPA client on remote environment deployment \(page 64\)](#)
- [DPA client Installation on a Virtual Desktop Infrastructure \(VDI\) \(page 65\)](#)
- [DPA client installation on other virtual environments \(page 65\)](#)
- [DPA client installation in Microsoft AppV \(page 65\)](#)
- [Verify DPA monitoring \(page 66\)](#)
- [DPA integration with various application types \(page 66\)](#)
- [Enable DPA to trigger on Terminal Emulators \(page 67\)](#)

Install the DPA client for citrix and terminal servers

Install the DPA client on a citrix server or a Windows server that hosts Terminal Services (TS) sessions. Perform the procedures below on each Citrix/Terminal Services server.

Prerequisite: Virtual channels permission

Permissions must be provided for Remote Desktop Services to control how users and groups access the server. For a description of the default permission types and detailed information about Remote Desktop Services permissions, see the documentation that accompanies the Remote Desktop Services Configuration administration tool.

If remote desktop/terminal services users are not given the permission "Virtual Channels," then the DPA session inside the remote session cannot communicate to the local session and the DPA session will not work correctly.

Similar permissions are required for DPA under Citrix environments.

Procedure

1. Install the DPA client on the Citrix or TS server according to the manual or silent installation instructions.
2. For 64-bit Citrix or TS Servers, ensure the EI BHO Plug-in is installed.
 - In manual installations, select Install IE BHO Plug-in
 - In silent installation scripts include USEIEBHO=Y

Citrix published applications

The DPA client command can be appended to existing published applications or set when publishing new applications.

There are two separate procedures that you can perform here. Perform one procedure if the published application is launched directly from the command line. Perform a separate procedure if the published application is launched by a script.

Published application launched from the command line

Procedure

1. If the published application is launched directly from the command line, add the following to the command line of each published application:

```
C:\<company_name>\DPA\Client\TsStart.exe <"path to executable">
```

Example:

```
N:\<company_name>\DPA\Client\TsStart.exe  
"C:\WINNT\System32\mspaint.exe"
```

Published application launched by a script

Procedure

1. If the published application is launched by a script, use TsStart within the script as follows:

Example:

```
@Echo off  
  
SET HOMEDRIVE=%USERPROFILE%  
  
N:\<company_name>\DPA\Client\TsStart.exe  
"C:\WINNT\System32\mspaint.exe"
```

The TsStart.exe always requires a command line parameter containing the path to the executable to be published. A call that includes TsStart.exe without a command line parameter containing the path to the executable to be published will not execute.

DPA client on remote environment deployment

DPA supports triggering and reporting when DPA is installed on a remote session or when DPA is installed both locally and remotely.

The remote session configuration items are enabled by default, and triggers that fire on the remote workstation must be defined with an additional %RUNONSERVER parameter.

Related Information

Remote DPA Sessions (*Desktop and Process Analytics User Guide*)

DPA client Installation on a Virtual Desktop Infrastructure (VDI)

To use the DPA client on a VDI environment, install the DPA client on the template VDI image.

To keep the DPA client data, make sure that the VDI image remains on and unchanged. That is, do not re-purpose, re-image, or shutdown the VDI image. Otherwise, the DPA client data is lost.



Regarding adherence tracking, the *User based No Activity* feature ensures that the end-of-shift notification is tracked in the VDI environment.

DPA client installation on other virtual environments

To use the DPA client on other virtual environments, install the DPA client on the virtual workstation template image.

To keep the DPA client data, make sure that the virtual workstation template image remains on and unchanged. That is, do not re-purpose, re-image, or shutdown the image. Otherwise, the DPA client data is lost.

If virtual channels feature does not exist, each template image acts as a separate data stream for the DPA client.

If virtual channels feature exists, it mimics either Citrix or terminal services virtual channels, and the data is merged against the local DPA client workstation.

DPA client installation in Microsoft AppV

To capture all triggers and application usage, install the DPA client **outside** of the Microsoft AppV Bubble.

Do not install DPA in AppV bubble either on its own or as part of an existing bubble. Installing DPA on AppV bubble is allowed only if DPA is required to monitor that one application or if for accessing an application API.

Accessing an API, such as *HLLAPI - High Level Language Application Program*, is used with Terminal emulators.

If DPA requires accessing an application API, you can install the DPA client in the AppV bubble for that application and configure it to only log trigger events for that application.

Global resource exclusions

As the application memory is virtual and DPA uses shared memory objects to communicate between its keyboard, mouse, and capture utilities, make sure to set the AppV to allow certain objects to be treated as **global** (rather than virtual).

Insert the string **Verint_*** as a global object exclusion to ensure memory resources are allowed for DPA.

Verify DPA monitoring

Run a timeline report to verify DPA is monitoring desktop activity and is activating event triggers.

Procedure

1. Ensure there is at least five minutes of application activity or event triggering on the desktop(s).
2. From **Desktop Process Analytics > Reports** menu, generate a **Timeline Report**.
3. Ensure the report contains data that correctly reflects the desktop activity.

Related information

Timeline Reports (*Desktop and Process Analytics User Guide*)

DPA integration with various application types

Deploying DPA allows detection of the window titles of all windows application without additional configuration. This section details those applications that require an additional level of integration for detection of objects inside the application's window.

Summary integration matrix

Application type	Support without integration	Support with specific integration	Supported integration type
Chrome V73+	Window title	Full control level support	Chrome store extension
Edge "Blink" V83+	Window title	Full control level support	Chrome store extension
Edge Non-Chrome (V37-42)	Window title	None	No further integration
Mozilla Firefox ESR 59 ONLY	Window title	Full control level support	Mozilla plugin from Verint KB
Mozilla Firefox >59	None	Window title and URL	Mozilla plugin from Verint KB
Embedded Chromium (CEF)	None	None	None
Java JRE	Window title only	Full field level controls	Access-bridge installation

Application type	Support without integration	Support with specific integration	Supported integration type
Terminal emulators	Window title only	Column and row coordinate data support	HLLAPI, COM
Python	Execute Python	Retrieve data from Python scripts into trigger variables	Python version 3.3, DCUApi enabled
WPF Embedded browser (WPFBROWSER)	Full field level controls through Accessibility support, CPU intensive	Internal object URL support, plus Full field level controls, optimized CPU	dll injection, DPA Validator option
Winforms Embedded browser (WINFORMBROWSER)	Full field level controls through Accessibility support, CPU intensive	Internal object URL support, plus Full field level controls, optimized CPU	dll injection, DPA Validator option
Embedded WebView Control (Edge)	None	None	None
SAPLPAD/SAPLOGON	Window title only	Full field level controls	SAPLPAD Scripting server and client side. Increases number of SAP connections to client due to use of SAP scripting channels
Windows forms applications	Full field level controls, CPU intensive	None	None

Enable DPA to trigger on Terminal Emulators

DPA and other third party applications can retrieve and view events from Terminal Emulators. To set up communication with the Terminal Emulator, use this procedure to ensure that the API file is included with the DPA client deployment.



Terminal Emulators or Green Screen applications typically present a connection to a legacy mainframe application as a fixed character width representation in 80x24 or 130x24 rows.

Typical TE API file names

Typically whllapi32.dll is the file name. The name may differ according to the environment.

Name	HllApiFileName	Typical HLL DLL Location
Host Explorer	whllapi32.dll	C:\Program Files (x86)\Hummingbird\Connectivity\13.00\HostExplorer
iSeries Access	whllapi32.dll	C:\Program files(x86)\IBM\Client Access\Emulator
iRumba	WHLLAPI.DLL	C:\Program Files(x86)\NetManage\RUMBA\System\
Passport	PassHll.dll	C:\Program Files(x86)\PASSPORT

Procedure

1. Copy the **whllap32.dll** file from the third party application directory, usually located in Program Files > TE_NAME.



As the file name differs according to the environment, it is best practice to search for *hl*.dll. If multiple files are returned, try each file until you can successfully capture screens.

2. Copy the **WHLLAPI32.dll** file into the same folder as the DPA client.
3. Rename the file to **WHLLAPI_pcmon.dll**.

Enable DPA to trigger events on web browsers

DPA supports triggering and collection of data from web browsers running on customer desktops. It is the customer's responsibility to deploy the plug-ins and to ensure it is not blocked or disabled after installation.

The DPA Validator uses the plug-ins when capturing browser screens and validating the screen controls. The DPA client uses the plug-in when invoking desktop activity triggers.

Related topics

[Enable DPA event triggers in Google Chrome \(page 69\)](#)

[Enable DPA Validator to capture Google Chrome screens \(page 69\)](#)

[Enable DPA window triggers in Mozilla Firefox \(page 70\)](#)

[Enable DPA in Java applications \(page 71\)](#)

[Enable DPA in SAPLGPAD/SAPLOGON applications \(page 71\)](#)

[Enable DPA integration in Kana web applications \(page 71\)](#)

Enable DPA event triggers in Google Chrome

The DPA chrome triggering plug-in is required to trigger events on Chrome browser screens.

Make sure to install and activate the DPA chrome triggering plug-in on all monitored desktops that are required to trigger events on Chrome browsers.

Enterprise deployment

The browser plug-in is developed according to the browser standards laid out by Google. To install the plug-in within an enterprise, consult the browser-specific guidelines as available from the software publisher.

Chrome plug-in location

The Chrome DPA event trigger is available from the Chrome store. When the Chrome store location is available, it is posted on the DPA User Wall. Until then, contact your software provider for the latest location.

i The Enterprise version of Google Chrome is required. If the correction version is not installed, you are prompted to install Chrome. To install the plug-in, you must first complete the installation.

Procedure

1. In Chrome web store, access the **Verint.dpa.chrome.trigger** plug-in.
<https://chrome.google.com/webstore/detail/verintdpachrometrigger/hlnipadenlamgabofnnpfkdgphfnjeh>
2. Click **Add to Chrome**.
3. On the **Add <extension_name>** dialog box, click **Add extension**.
The extension is installed.
4. Verify that the extension is listed on the Extensions page by typing the following address:
chrome://extensions//
5. Close the browser.

Related information

Deploy Chrome for Work on Windows

(<https://support.google.com/chrome/a/answer/3115278?hl=en>)

Enable DPA Validator to capture Google Chrome screens

The DPA Validator chrome plug-in is required to capture and validate Chrome browser screens.

Make sure to install and activate the DPA Validator chrome plug-in only on computers used to validate screens.

Chrome plugin location

The Chrome DPA Validator plug-in is available from the Chrome store. When the Chrome store location is available, it is posted on the DPA User Wall. Until then, contact your software provider for the latest location.

Procedure

1. Access the **Verint.dpa.chrome.validator** plug-in in the Chrome web store.
<https://chrome.google.com/webstore/detail/verintdpachromevalidator/gofohnjbcabckdcbamaelhmpjjoegikd>
2. Click **Add to Chrome**.
3. On the **Add <extension_name>** dialog box, click **Add extension**.
The extension is installed.
4. Verify that the extension is listed on the Extensions page by typing the following address:
chrome://extensions//
5. Close the browser.
6. To capture a screen:
 - a. Open **Validator**.
 - b. Open the Chrome page you want to capture.

Related information

Deploy Chrome for Work on Windows

(<https://support.google.com/chrome/a/answer/3115278?hl=en>)

Enable DPA window triggers in Mozilla Firefox

DPA deploys a Mozilla Firefox plug-in (V60 and above) for the detection of URL and window titles within Firefox browsers. While window triggers can be configured on specific URL or window titles, screen content triggers are not supported with Mozilla Firefox.

Enterprise deployment

The browser plug-in is developed according to the browser standards laid out by Mozilla. To install the plug-ins within an enterprise, consult browser-specific guidelines as available from the software publisher.

Firefox plug-in location

The **DPA Firefox plug-in** is available from the **Latest Desktop Components for: <version>** page.

Procedure

1. Download the **DPA Firefox Plug-in** KB, and then extract it to a directory on the target desktop.
2. In Firefox, go to the **about:addons** address.
3. In the left pane, click **Extensions**.

4. Drag the relevant extracted DPA xpi files to the center of the extensions page.
5. Confirm the installation.

Related topics

[Obtain the installation packages \(page 18\)](#)

Related information

Deploying and configuring Firefox within an enterprise (<https://support.mozilla.org/en-US/products/firefox-enterprise>)

Enable DPA in Java applications

DPA uses the Java accessibility components to integrate into Java applications. If DPA Validator reports the captured application as JAVA, JAVAW, or JRE, the underlying application is a Java virtual workstation. Typically, JRE is deployed without its *Access Bridge* accessibility feature enabled. When the feature is enabled, DPA can validate Java applications and run triggers based on Java field level controls.

Related information

Enabling Java Access Bridge (https://docs.oracle.com/javase/7/docs/technotes/guides/access/enable_and_test.html)

Enable DPA in SAPLGPAD/SAPLOGON applications

DPA uses the SAP automation components to integrate into SAP *Thick Client* applications. If DPA Validator reports the application as SAPLGPAD or SAPLOGON, the underlying application runs in an SAP product environment.

SAP is often deployed without the SAP automation feature enabled. When the feature is enabled, DPA can validate SAP applications and run triggers based on SAP field level controls.

Related information

See <http://help.sap.com> for information on SAP GUI scripting

Enable DPA integration in Kana web applications

To enable DPA to capture screens from Kana web applications, select the **Use Auto ID Match** option in the validator setting of the Kana Engagement Management.

DPA public-private token authentication

Desktop and Process Analytics (DPA) uses token and header authentication processes to validate DPA applications and screen captures. Authentication key management is the customer's responsibility.

Purpose of DPA authentication

The purpose of the DPA authentication process is to:

- Ensure that the DPA client sends data from valid applications on the desktop to Avaya Experience Platform™ Workforce Engagement.
- Ensure that the DPA Validator can upload screens from the desktop to Avaya Experience Platform™ Workforce Engagement. for DPA trigger definition.
- Ensure that the DPA Process Discovery client (Visio plugin) can retrieve data from Avaya Experience Platform™ Workforce Engagement.

DPA authentication does not prevent packet sniffing from finding out what is in the data (TLS will combat this), nor does it prevent data-at-rest on the client from being in text format (encryption of data -at-rest will combat this).

Related topics

[Prepare DPA authentication keys \(page 72\)](#)

[Modify DPA authentication keys \(page 74\)](#)

Related information

DPA data flows are documented in the *Technical Overview Guide*.

Prepare DPA authentication keys

The DPA client and server authentication keys must comply with RSA XML formats. The file names, length and format are outlined here. Prepare the key

Key file names

Ensure the client and server paired XML file names are:

- verint_dpa_client.xml
- verint_dpa_server.xml

Key length

The default key provided with the DPA installation is 1024-bit length. The system supports keys in length from 384-bits to 16384-bits.

DPA client public key

The client side of the key is not site specific and is included within the DPA client installer.

The folder key location on the client is %PROGRAMDATA%\Avaya\DPA\Keys\verint_dpa_client.xml

Key registry file

The key file is stored in the local workstation's registry.

- Registry location: HKEY_LOCAL_MACHINE\SOFTWARE\Verint\DPA
- String key: KeyFile
- Value: full path to the XML file containing the DPA client authentication key.

DPA server private key

The server portion of the key is deployed during system installation.

The folder key location on the server is %IMPACT360DATADIR%\keys\verint_dpa_server.xml

Private/Server key format

The private key XML file must conform to the following format:

```
<RSAKeyValue>
  <Modulus>...</Modulus>
  <Exponent>...</Exponent>
  <P>...</P>
  <Q>...</Q>
  <DP>...</DP>
  <DQ>...</DQ>
  <InverseQ>...</InverseQ>
  <D>...</D>
</RSAKeyValue>
```

Public/Client key format

The public key XML file must conform to the following format:

```
<RSAKeyValue>
  <Modulus>...</Modulus>
  <Exponent>...</Exponent>
</RSAKeyValue>
```

Key parameters

Parameter	Description
Modulus	Modulus of key
Exponent	Exponent of key
P	PrimeP
Q	PrimeQ
DP	PrimeExponentP
DQ	PrimeExponentQ
InverseQ	CrCoefficient
D	PrivateExponent

Related information

Microsoft article: [Create and return an XML string containing the key of the current RSA object](#)

Modify DPA authentication keys

To modify DPA authentication keys, contact Verint.

Uninstall/rollback DPA clients

You can remove (uninstall) the DPA client, or rollback/repair to an earlier version of the 15.2 DPA client. Remove the later version and then rollback/repair to the desired client version.

Example:

The desktops are installed with revisions A, B, and C of the 15.2 DPA clients. If you want to rollback to revision A, the process is as follows:

1. Uninstall revision C.
2. Uninstall revision B.
3. Rollback / repair revision A.

Related topics

[Uninstall and rollback DPA client using the original msi \(page 75\)](#)

[Uninstall and rollback DPA clients using a script \(page 75\)](#)

[Uninstall a DPA client through add/remove programs \(page 76\)](#)

Uninstall and rollback DPA client using the original msi

Remove or rollback the DPA client by executing the original MSI used to install the DPA client.

Procedure

1. Log on to the workstation with administrative rights. If required, elevate the UAC security.
2. Browse to **<DPA setup files location>\SetupDir\Client_MSI_Install**.
3. Double click to run the installer:
 - For a desktop with 32-bit operating system, run **PCMONClient.msi**
 - For a desktop with 64-bit operating system, run **PCMONClient64.msi**
4. In the **Welcome** screen click **Next**.
5. Select the **Remove/Repair** option.
6. For repair, select the client version to rollback to.

Uninstall and rollback DPA clients using a script

Remove and rollback the DPA client by executing a script.

Procedure

1. To uninstall the DPA client, run one of the following scripts:
msiexec /x PCMONClient.msi /q /n /norestart
msiexec /x PCMONClient64.msi /q /n /norestart
2. To uninstall when you do not have the original installer, run the following script:
msiexec /x {productcodegoeshere} /q /n /norestart
3. To rollback/repair the DPA client, run one of the following scripts:
msiexec /fmasu PCMONClient.msi /q /n /norestart
msiexec /fmasu PCMONClient64.msi /q /n /norestart
4. To rollback/repair when you do not have the original installer, run the following script:
msiexec /fmasu {productcodegoeshere} /q /n /norestart

Product code

The product code is taken from the from the pcmonclient.html file of the previous installer or from the registry of a target workstation with the client installed. It is the same for all MSI versions. The brackets {} around the product code are required.

Uninstall a DPA client through add/remove programs

To remove the DPA client through Add/Remove Programs, the original MSI is not required.

Procedure

1. From **Start > Settings > Control Panel**, open **Add or Remove Programs**.
2. Select the **DPA Client** option.
3. Select the **Remove** option.

Install DPA Validator

The DPA Validator utility captures screens, validates screen controls, and displays the screen inside the utility for the user to browse and select controls to be used when defining trigger events.

DPA Validator interface language

It is possible to change the interface language from the default English (US) to any licensed language. A DPA database plugin sends licensed language information from the server to the local ValidatorLanguages.xml file that is included with the installation files.

DPA Validator output

The validator uploads a bitmap image file, and an XML data file containing the screen control meta data. The image and data file can be accessed from the DPA Screen Library during trigger definition.

Before you begin

- Verify if you require the 32-bit version or 64-bit version of the utility.
- Delete sensitive data on the screen, prior to capturing the screen.
- To ensure that you have the latest software, get the utility from the portal, or use the **Add New Screen** option in the DPA Trigger module.

Procedure

1. To launch the Setup Wizard, do one of the following:
 - (recommended) If downloaded from the portal, extract the KB<number>.zip. Ensure all files are extracted to the same folder.
 - Double-click **DPAValidator32.exe** or **DPAValidator64.exe**.
2. To retrieve an existing capture, click **Open** and browse for the image file.
3. To capture a new screen, open **Settings** to define the capture settings.
4. To change the interface language, select a **Language** from the list.
5. Click **OK** to save the capture settings, and then click **Capture**.
6. Select the target screen to bring it in to the foreground. Wait for an image of the screen to appear in the **Capture** tab.

7. Use the **Search** and **Find** options to browse for screen controls.
 - Select **Search Selected Controls** to browse controls already selected.
 - Clear **Search Selected Controls** to browse all available controls.
 - To search for controls with a specific name or value, use **Find Controls**.
8. Select controls that are highlighted in red. The control is assigned a reference number.
9. In the **Save & Upload** tab, enter the upload settings, and **Save** the screen.
10. If required, [Enable DPA Validator to capture Google Chrome screens \(page 69\)](#).

Related information

Working with the DPA Validator (*Desktop and Process Analytics (DPA) User Guide*)

Add a New Screen (*Desktop and Process Analytics (DPA) User Guide*)

DPA Process Discovery

DPA Process Discovery Client is a Visio based reporting tool for DPA Analysts. It is a plug-in for Microsoft Office Visio that generates workflow visualization on DPA event trigger and DPA application process data.

Process Discovery provides a means to discover workflow variations between users and to visualize these workflows as Microsoft Visio diagrams.

This installation is typically performed by a DPA Analyst.

Related topics

[Install Process Discovery \(page 78\)](#)

[Add Process Discovery Menu to Microsoft Office Visio \(page 79\)](#)

[Process Discovery silent install parameters \(page 79\)](#)

Install Process Discovery

To use the DPA Process Discovery client in visio, you must first install the Process Discovery msi.

Before you begin

- Meet all hardware and software specifications.
- Download the Process Discovery installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. To launch the Setup Wizard, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.OR
 - If installing from the media, run the **ProcessDiscoverySetup.msi** as an administrator.
2. When the installation of the prerequisites completes, a message to reboot the desktop is displayed. Click **Yes** to reboot.
3. On the **Process Discovery Welcome** page, click **Next**.
4. Accept the End User License Agreement.
5. On the **Select Installation Folder** page, select an installation folder and click **Next**.
Default destination folder: C:\Program Files\<company_name>\Process Discovery\.
6. On the **Enter DPA Webservice url** page, enter the name of the Application Load Balancer, and then click **Next**.

7. On the **Confirm Installation** page, click **Next**.
8. On the **Installation Complete** page, click **Close**.

What to do next

[Add Process Discovery Menu to Microsoft Office Visio \(page 79\)](#)

Add Process Discovery Menu to Microsoft Office Visio

After installing the DPA Process Discovery msi, you are ready to add the Process Discovery menu to Microsoft Office Visio.



Process Discovery is also supported in Microsoft Office 365.

Procedure

1. Open Microsoft Office Visio.
2. In the Microsoft Office Customization Installer window, click **Install**.
A new Process Discovery menu appears in Visio.

Process Discovery silent install parameters

The properties determine how Discovery Process is installed silently on the desktops.

Parameters	Description and Default Values
MsiFile	Installation file name: ProcessDiscoverySetup.msi
MSIS_DIR	Installation file location. Typically: <Shared network folder:>\DesktopApplications
INSTALLDIR	Installation folder destination. Default: c:\Program Files\Verint\Process Discovery\
USEHTTPS	Communication protocol. USEHTTPS=Y - DPA client uses HTTPS to support TLS USEHTTPS=N - (default) DPA client uses HTTP
PDSERVER	Application Load Balancer address.
WEBSERVICEURL	Process Discovery service URL. http(s)://<Application Load Balancer address>/DPAProcessServices/DataAnalyzerService.svc

Related topics

For a sample script that includes the command line for distributing this application in silent mode, see [Installation by role: silent distribution \(page 36\)](#)

Form Designer

The Form Designer is used for designing evaluation and assessment forms. This section contains the information required to install the Form Designer.

Related topics

For all software and hardware specifications refer to [Customer requirements \(page 19\)](#).

Install Form Designer manually

The Form Designer application requires the mandatory resources contained in Desktop Resources.

Before you begin

- Install [Desktop Resources \(page 47\)](#)
- Download the Form Designer installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. To launch the Installation Wizard, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.
 - OR
 - If installing from the media, double-click **FormDesignerInstallation.msi**.
- The installation of Form Designer requires Administrator privileges. If you don't have these privileges, a pop-up window will appear before the Installation Wizard runs, asking you for your Elevated User Details.
2. On the **Welcome** page, click **Next**.
 3. On the **End-User License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
 4. To view the required space for an application, on the **Custom Setup** page, select it in the list and read the text in the pane on the right. Click **Next**.
 5. If a list of missing prerequisites appears, click **Close** and then click **Cancel**. Install the missing prerequisites and restart the installation.
When there are no missing prerequisites, the **General Settings** page appears.
 6. Enter the alias of the Application Load Balancer.

7. If a third-party Identify Provider is used, select **Authentication using third-party IdP** and enter the alias of the IdP server.
8. (Optional) To enable HTTPS, select **Use HTTPS for client/server communication**.
9. If upgrading from a V11 system, select **Upgrade from V11 system** and enter the authentication URL port and application URL port for communicating with the Application Load Balancer during the upgrade (default ports 7002/443).



This setting is only used during the upgrade phase to enable communication between a V15.2 desktop and a V11 Data Center. If the Data Center is already upgraded to V15.2, this setting is ignored. See [Port usage during upgrade](#), page 1.

10. Click **Next**.
11. On the **Ready to Install** page, click **Install**.
12. When the installation is complete, the **InstallShield Wizard Completed** page appears. Click **Finish**.
The **Installer Information** message appears prompting you to restart the computer.
13. Restart your computer.
14. On the **Ready to Install** page, click **Install**.
15. When the installation is complete, the **InstallShield Wizard Completed** page appears. Click **Finish**.
The **Installer Information** message appears prompting you to restart the computer.
16. Restart your computer.

Form Designer silent install parameters

The properties determine how Form Designer is silently configured.

Parameters	Description and Default Values
MsiFile	FormDesignerInstallation.msi
VERINTFOLDER	Installation folder destination
USE_COMMAND_LINE	USE_COMMAND_LINE=1 Mandatory
GLOBAL_APP_SERVER_DNS	Application Load Balancer address Mandatory

Parameters	Description and Default Values
GLOBAL_APP_SERVER_AUTH_PORT	Application Load Balancer port For new installations, leave blank. Default port is 443. For gradual upgrades, in which the desktop application communicates with the previous Data Center version, set the actual port of the Application Load Balancer (default = 7002).
GLOBAL_APP_SERVER_IIS_PORT	Default = 443
GLOBAL_USE_SSL	1 = Use TLS Default = 1
TERMINAL_SERVER	0 = No Terminal server 1 = Terminal server mode Default = Auto detect

Related topics

See [Installation by role: silent distribution \(page 36\)](#) for a sample script that includes the command line for distributing this application in silent mode.

Logger

Installing the Logger provides the infrastructure for the Desktop Applications to generate logs. Log severity and destination defaults can be modified for troubleshooting purposes by using the Logger Manager. Logs can be viewed using the Logger Viewer.

Related topics

For all software and hardware specifications refer to [Customer requirements \(page 19\)](#).

Install Logger manually

The manual Logger installation procedure must be performed on the desktop on which the application will run. This application requires the mandatory resources contained in Desktop Resources.

Before you begin

- Install [Desktop Resources \(page 47\)](#)
- Download the Logger installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. To launch the Installation Wizard, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.
 - OR
 - If installing from the media, double-click **LoggerInstallation.msi**.
2. On the **Welcome** page, click **Next**.
3. On the **End-User License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
4. To view the required space for an application, on the **Custom Setup** page, select it in the list and read the text in the pane on the right. Click **Next**.
5. If a list of missing prerequisites appears, click **Close** and then click **Cancel**. Install the missing prerequisites and restart the installation.
When there are no missing prerequisites, the **Ready to Install** page appears.
6. On the **Ready to Install** page, click **Install**.
7. When the installation is complete, the **InstallShield Wizard Completed** page appears. Click **Finish**.
The **Installer Information** message appears prompting you to restart the computer.
8. Restart your computer.

Logger silent install parameters

The properties determine how Logger is configured silently on the agent desktops.

Basic Parameters	Description and Default Values
MsiFile	LoggerInstallation.msi
USE_COMMAND_LINE	USE_COMMAND_LINE=1 Mandatory
INSTALLFOLDER	Specifies the installation destination

Related topics

Refer to [Installation by role: silent distribution \(page 36\)](#) for a sample script that includes the command line for distributing this application in silent mode.

Player

The Player enables users to listen to audio and view recorded screen activity and video playback, change the volume or speed of a call, jump to different points in a call, and see the waveform for an interaction.

Types of Players

There are two types of players:

- Streaming Player (does not require installation on the client workstation)
- Plugin Player

Plugin Player installation considerations

The Plugin Player installation package incorporates codecs and infrastructure for the playback controls.

The Plugin Player installation package also contains the Legacy Playback application. It enables playing media from a legacy system in upgrade scenarios, and for verifying archive media in the Central Archive Manager (CAM).

The latest Plugin Player application can be installed side-by-side with the existing Legacy Playback application.

For all software and hardware specifications refer to [Customer requirements \(page 19\)](#).

Related topics

- [Install the Plugin Player manually \(page 86\)](#)
- [Silent install parameters for Plugin Player \(page 89\)](#)
- [Enable real time playback of encrypted screen content in transit \(page 91\)](#)
- [Configure stereo recorded contact playback as mono \(page 91\)](#)
- [Configure volume amplification \(page 93\)](#)
- [Video playback tuning \(page 94\)](#)
- [Configure network adapters for real-time audio playback in plugin Player \(page 95\)](#)

Install the Plugin Player manually

Ensure all site preparation and system requirements are met before proceeding with the Plugin Player installation instructions. This application requires the mandatory resources contained in Desktop Resources.

Before you begin

- Install [Desktop Resources \(page 47\)](#)
- Download the Plugin Player installation package, according to [Obtain the installation packages \(page 18\)](#).

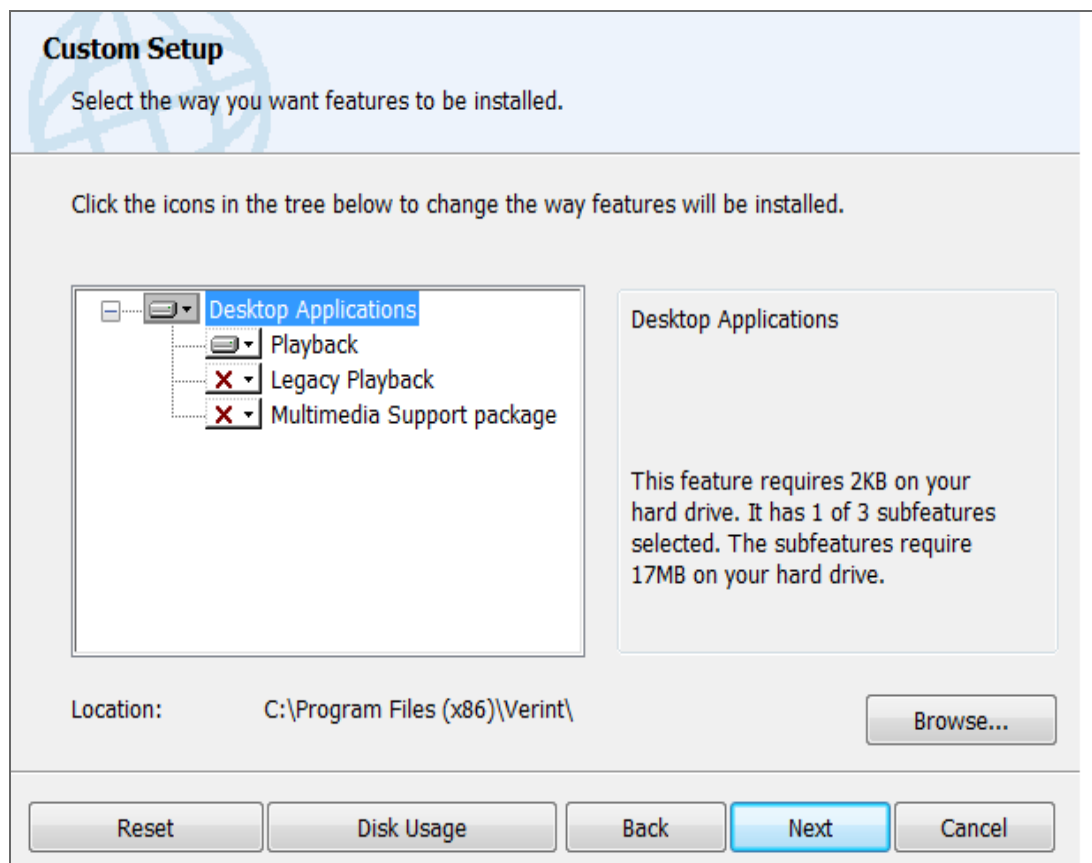


To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. If a previous version of the Plugin Player is installed, remove it through Windows Control Panel.
2. To launch the Installation Wizard, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.
 - OR
 - If installing from the media, double-click **PlaybackInstallation.msi**.
3. On the **Welcome** page, click **Next**.
4. On the **End-User License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.

The **Custom Setup** page appears.



5. On the **Custom Setup** page, select the relevant features to install:
 - For a new installation:

Keep the default, **Playback** only. This option enables the Player in 15.2 systems. It is not required to make the Multimedia Support Package available for installation as the Plugin Player incorporates this package and installs it automatically.
 - For upgrade:

If upgrading from V11.2 and higher, keep the default which is **Playback**.
If upgrading from earlier versions such as V11.x, to enable the Player:
 - Select **Playback** and **Legacy Playback**.
 - Expand **Legacy Playback** and select **Will be installed on local hard drive**.
- For downloaded media files:

Select only the **MultiMedia Support Package** option (clear the other options). Relevant when downloading audio files for playback on workstations outside the enterprise or on workstations that do not have access to the Portal Player.

 - Expand **Playback** and select **Entire feature will be unavailable**.
 - Expand **MultiMedia Support Package** and select **Will be installed on local hard drive**.
6. Select additional options as required:
 - **Browse**: Click **Browse** to change the default destination folder. The **Browse** button is enabled when **Desktop Applications** is selected.
 - **Reset**: Click **Reset** to revert to the default installation settings.
 - **Disk Usage**: Click **Disk Usage** to view the disk space required compared to the disk space on the destination drives.
7. Click **Next**.
8. If a list of missing prerequisites appears, click **Close** and then click **Cancel**. Install the prerequisite software and resume the installation.

When there are no missing prerequisites, the **Playback Settings** page appears.
9. Set the playback encryption as follows:



The Encrypted Playback setting is required if a supervisor will download the encrypted file and then play back the file using Windows Media Player (WMP).

10. Select **Encrypted Playback**.
11. In the **Data Center Address** field, enter the Application Load Balancer address.
12. Click **Next**.
13. On the **Ready to install Playback** page, click **Install**.
14. When the installation is complete, the **InstallShield Wizard Completed** page appears. Click **Finish**.

The **Installer Information** message appears prompting you to restart the computer.

15. Restart your computer.



Playback is supported in thin-client environments. However, due to delay in playback of audio between the CITRIX or Terminal Server and its client, the audio quality could be reduced. To overcome this, reduce the buffering of audio on the client side. However, it is important to understand that there could still be some reduction in the quality of playback.

Silent install parameters for Plugin Player

The properties determine the configuration of the Plugin Player in silent installation on the client workstations.

Parameters

Parameters	Description and Default Values
MsiFile	Installation file name: PlaybackInstallation.msi
USE_COMMAND_LINE	Use command line. Mandatory USE_COMMAND_LINE=1
INSTALLFOLDER	Installation folder destination.
PLAYBACK_ENCRYPTED	Playback of encrypted media (audio and screen files) must be enabled. 1 - Enable playing encrypted media
PLAYBACK_ENCRYPTIONWEBSERVICE	Application Load Balancer alias name. If PLAYBACK_ENCRYPTED is set to 1, this setting is mandatory. Default=Empty
ADDLOCAL	Legacy Player is installed locally. The legacy Player is required in upgrade scenarios to play media from previous versions. <ul style="list-style-type: none"> For new installations: ADDLOCAL=Playback (default) To support playback of media from all versions on the same desktop: ADDLOCAL=ALL To enable playback in Windows Media Player (install the codec pack without the actual Player): ADDLOCAL=MultimediaSupportPackage

Parameters	Description and Default Values
SSL	Security setting. Mandatory, if PLAYBACK_ENCRYPTED is set to 1, or when data-at-rest encryption is enabled. SSL=1 (default) to support TLS SSL=0 does not support TLS
PORT	Port number for accessing a previous Data Center version after upgrade. Mandatory, if PLAYBACK_ENCRYPTED is set to 1, or when data-at-rest encryption is enabled. Default = 7002
USEOLDVIDEORENDERER	Video renderer type. 0 - Default video renderer is used (EVR) (default) 1 - Old video renderer (VMR7) is used Note: This parameter is used only in rare cases . Consult with Verint.

Related topics

For a sample script that includes the command line for distributing this application in silent mode, see [Installation by role: silent distribution \(page 36\)](#).

Playback without Portal

When playback of audio files recorded by the system is required by users that do not have access to the Search Interactions and Forms page, including users outside the enterprise, several methods can be used to playback the audio files.



Only decrypted files should be sent outside the enterprise, as playback of encrypted files requires login to the Search Interactions and Forms page.

Methods used to playback audio files

- **Download in Standard Windows format:** An enterprise user downloads audio files from the Portal in the standard Windows codec format and sends them to the external user.
- **Download in proprietary compressed format and supply the user with the relevant codec (Multimedia Support Package):** An enterprise user downloads audio files from the Portal in the proprietary codec format, sends them to the external user, and supplies the external user with the Playback.msi for installing the Multimedia Support Package.
- **Download in Proprietary Format and convert to standard Windows format:** An enterprise user downloads audio files from the Portal in the proprietary codec format, converts them to a standard Windows codec file using the Media Encoder, and then sends the converted audio files to external user.

Related topics

For detailed information on the Media Encoder, see [Media Encoder \(page 191\)](#).

Enable real time playback of encrypted screen content in transit

You can enable real time playback of encrypted screen content in transit from the supervisor desktop.

Procedure

1. Obtain the **client.wss** file.
2. Save the file for the supervisor desktop in the installation folder.

Default: C:\Program Files\<Company Name>

Related information

Generate screen encryption security files (*Security Configuration Guide*)

Configure stereo recorded contact playback as mono

When using the plugin Player, you can configure the system to play back stereo recorded contacts as mono recorded contacts by adding a dedicated registry key.

Enable stereo playback as mono

When stereo playback as mono is enabled, the audio waveform continues to show the color-coded speaker separation, but you cannot control the volume of each speaker separately.

Procedure

1. Open Notepad.
2. Depending on the operating system, copy the appropriate content into Notepad:

- For 32-bit operating systems:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai]

"MonoToStereo"=dword:00000001

- For 64-bit operating systems:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai]

"MonoToStereo"=dword:00000001

3. Save the file as *.reg (this file must be saved in *.reg file format).

4. Locate the file you created in step 3, and double-click it.
A confirmation message appears.
5. Click **Yes**.

Disable stereo playback as mono

You can temporarily disable stereo playback as mono by assigning a null value to the **MonoToStereo** key in the registry. Or, you can remove the key from the registry.

Procedure

1. Open Notepad.
2. Do one of the following:
 - To disable by changing the value of the registry key, go to Step 3.
 - To disable by deleting the registry key, Step 4.
3. Do the following to *change the value* of the **MonoToStereo** registry key:
 - a. Depending on the operating system, copy and paste the appropriate content into Notepad:
 - For 32-bit operating systems:
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai]
"MonoToStereo"=dword:00000000
 - For 64-bit operating systems:
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai]
"MonoToStereo"=dword:00000000
 - b. Save the file as *.reg (this file must be saved in *.reg file format).
 - c. Locate the file you created in step b, and double-click it.
A confirmation message appears.
 - d. Click **Yes**.
4. Do the following to *remove* the **MonoToStereo** key from the registry:
 - a. Go to **Start > Run**, and type **Regedit**.
 - b. Depending on the operating system, locate the correct registry:
 - For 32-bit operating systems:
[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai]
 - For 64-bit operating systems:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai]
 - c. Right-click the **MonoToStereo** key, and select **Delete**.

Configure volume amplification

When using the plugin Player, you can increase the playback volume on the portal by configuring the amplification level in the registry. This feature is useful when the maximum volume of the playback is not sufficient.

Enable volume amplification

When volume amplification is enabled, you can increase the volume of the playback up to the configured amplification level. Increasing the amplification level may reduce the sound quality. For stereo playback, the amplification is done for each channel separately.

Procedure

1. Open Notepad.
2. Depending on the operating system, copy the appropriate content into Notepad:
 - For 32-bit operating systems:
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai]
"AmplifySound"=dword:00000190
 - For 64-bit operating systems:
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai]
"AmplifySound"=dword:00000190
AmplifySound value is the amplification percentage in Hexadecimal.
0x00000190 equals to 400%. The available range is from 100%-800%. Setting a value larger than 400% may reduce the sound quality.
3. Save the file as *.reg (this file must be saved in *.reg file format).
4. Locate the file you created in step 3, and double-click it.
A confirmation message appears.
5. Click **Yes**.

Disable volume amplification

You can temporarily disable volume amplification by assigning a null value to the **AmplifySound** key in the registry. Or, you can remove the key from the registry.

Procedure

1. Open Notepad.
2. Do one of the following:
 - To disable by changing the value of the registry key, go to Step 3.
 - To disable by deleting the registry key, Step 4.
3. Do the following to *change the value* of the **AmplifySound** registry key:
 - a. Depending on the operating system, copy and paste the appropriate content into Notepad:
 - For 32-bit operating systems:
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai]
"AmplifySound"=dword:00000000
 - For 64-bit operating systems:
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai]
"AmplifySound"=dword:00000000
 - b. Save the file as *.reg (this file must be saved in *.reg file format).
 - c. Locate the file you created in step 3, and double-click it.
A confirmation message appears.
 - d. Click **Yes**.
4. Do the following to *remove* the **AmplifySound** key from the registry:
 - a. Go to **Start > Run**, and type **Regedit**.
 - b. Depending on the operating system, locate the correct registry:
 - For 32-bit operating systems:
[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai]
 - For 64-bit operating systems:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai]
 - c. Right-click the **AmplifySound** key, and select **Delete**.

Video playback tuning

After activating the McAfee Host Intrusion Prevention feature (HIPS) out of the box, video replay can be slow and consume CPU. The reason is that HIPS analyzes the video stream, as part of the standard

process.

To prevent HIPS from analyzing the video stream, turn on the HIPS adaptive mode feature. This feature ensures that the system identifies the video stream as a standard video stream and not as a threat. After the feature is turned on, the system creates a rule to prevent it from analyzing the video stream.

After the rule is added to the standard policy, adaptive mode can be turned off, and video playback works smoothly.

Configure network adapters for real-time audio playback in plugin Player

During real-time monitoring, in order for the recorder to send the audio stream to the Player, the Player must provide the recorder with the IP of the desktop.

When performing real-time monitoring from a desktop with a plugin Player, if audio is not working and you have identified that the IP sent to the recorder is incorrect, you must configure your network adapter so that the Player retrieves the correct IP.

In the desktop registry, add a RealtimeIPFilter description for the network adapter. The Player searches for the network adapter that matches the RealtimeIPFilter description and uses the IP associated with the network adapter to send to the recorder.

If the desktop uses more than one network adapter to connect to the network, you can set a description for each one (for example, RealtimeIPFilter, RealtimeIPFilter1, RealtimeIPFilter2). If no IP is associated with RealtimeIPFilter, the Player searches for an IP associated with RealtimeIPFilter1, and so on.

The Player stops searching if an IP is found or if there are no more network adapters that match the RealtimeIPFilter description. If no IP can be found, the Player uses a random IP.

Procedure

1. To obtain a list of all available adapters, open a command line and run:
ipconfig /all
2. Go to:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai (for 64bit desktops)
HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai (for 32bit desktops).
3. Add a string **RealtimeIPFilter** and set the following:
 - Value name = RealtimeIPFilter
 - Value data = the adapter's description (or part of it)
For example, Cisco AnyConnect.
4. To add a description for additional network adapters, set the value names to RealtimeIPFilter1, RealtimeIPFilter 2, and so on.

Configure the Player to improve screen playback performance

When playing back screens in the plugin Player, playback performance issues may occur. For example, the screen recording sometimes lags behind the audio recording. To improve the screen playback performance, you can configure the frequency at which the Player displays frames. If the interval between frames is increased, the screen playback performance improves. However, this may affect the screen quality.

If you encounter screen playback performance issues, we recommend setting the milliseconds between frames between 200 to 500 milliseconds. This outputs 5 or 2 frames per second, respectively.

Procedure

1. Go to **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai**.
2. Add a **DWORD** value named **millisBetweenFrames**.
3. Set this new value to **200** to show **5 frames per second**, or to **500** to show **2 frames per second**.

Phonetics Boosting

The Speech Recognition engine recognizes terms and phrases in the language models integrated with the Speech Analytics application. Through Phonetics Boosting, you can enhance the vocabulary of the default language model by adding terms and phrases that are part of your company's line of business. Adding these terms boosts their recognition, making them more effective in searches, categories, and trends.

For all software and hardware specifications refer to [Customer requirements \(page 19\)](#). The desktop must have at least 500 MB of free RAM space.

Related information

Phonetics Boosting User Guide

Install Phonetics Boosting manually

The Phonetics Boosting installation procedure must be performed on the desktop on which the Phonetics Boosting application is run. This application requires the mandatory resources contained in Desktop Resources.

Before you begin

- Install [Desktop Resources \(page 47\)](#).
- Download the Phonetics Boosting installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. To launch the Installation Wizard, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.
 - OR
 - If installing from the media, double-click **PhoneticsBoostingAppDesktopWix.msi**.
2. On the **Welcome** page, click **Next**.
3. On the **End-User License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
4. On the **Custom Setup** page, click **Next**.
5. On the **Ready to Install Phonetics Boosting Application** page, click **Install**.
The **Installing Phonetics Boosting Application** page appears.
6. Click **Next**, once the Setup Wizard completes the Phonetics Boosting installation.
The Completed the Phonetics Boosting Application Setup Wizard window appears.

7. Click **Finish**.

The Phonetics Boosting applications is installed successfully.

Screen Capture and AIM

Screen Capture and AIM includes three main components.

Screen Capture and AIM components

- **Capture Service:** Manages the starting and stopping of the Screen Capture Program. Communicates with the Recorder to track agent login and logoff events both on an agent's desktop PC or a Terminal Session and notifies the Integration Service of these events.
- **Screen Capture Program:** On request from the Recorder, this component captures screen changes from a desktop PC or Terminal Session and forwards the changes to the Recorder where they are saved into a file.
- **Agent Initiated Monitoring (AIM):** Enables the agent to control the recording process by issuing Start/Stop/Pause/Resume/Block Monitor Parameters. Installation of AIM is optional.

Screen capture proxy

For real-time playback on the Chrome, Edge, or Safari browser, the screen capture proxy service uses a Verint signed certificate.

Related topics

[Customer requirements \(page 19\).](#)

Related information

AIM Quick Reference Guide

AIM Online Help

Install Screen Capture and AIM manually

You can use the instructions to perform a manual installation on an **agent workstation, a Terminal Server, a Citrix server, or a Virtual workstation**. The installation pages that appear when installing on a Terminal Server or Citrix server are slightly different than those that appear when installing on an agent workstation. The differences are noted in the installation procedure.

Supported operating systems

In addition to the operating systems listed in [Supported operating systems \(page 20\)](#), the Screen Capture Agent also supports Windows 11.

Installation location

If Selective Screen Application Recording will be used, install the Screen Capture Agent software in \Program Files (x86).

Before you begin

- Download the latest Screen Capture and AIM installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

- If installing in the Azure cloud with Azure Virtual Desktop, the Screen Capture module must be installed using administrative privileges. The software is installed once per Azure Virtual Desktop multi-session host.

Procedure

1. To install Screen Capture and AIM, do one of the following:
 - (recommended) If downloaded from the portal, open the command prompt and run as administrator the **KB<number>.msi**.
 - OR
 - If installing from the media, right-click **Screen_Capture_Module.exe**, and then click **Run as administrator**.
2. On the **Welcome** page, click **Next**.
3. On the **End-User License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
4. (Terminal Services or Citrix environments only). On the **Terminal Services configuration** page, complete the Quality Monitoring Server configuration.
 - a. In the **Enter your BDR Server Name and Port Number** field, enter the Integration Service hostname and port number.
Format: <Integration_Service_hostname>:<port>
 - b. Click **Next**.
5. (Upgrades only). On the **Upgrade Processing** page, click **Next**.
6. On the **Destination Folder** page, accept the defaults or click **Change** to select different destination folders for the Screen Capture software and its log files. Then click **Next**.
7. (Optional) On the **Data Security** page,
 - a. Select **Send FQDN** for the Screen Capture Agent to send the Fully Qualified Domain Name (FQDN) to the Recorder Integration Service and Recorder.
 - b. Click **Next**.
8. On the **Integration Services Options** page, to operate with Recorder servers or in an Avaya Contact Recorder environment, select one of the following:
 - The **Connect to Integration Services (Legacy)** is shown for reference but is not available for editing.
 - To connect the Capture Service on the desktop with a **secured** connection to the Integration Service, select **Connect to Secure Integration Services**.
Enter the Integration Service host name and port number. A maximum of eight (8) hosts can be added. Separate entries with a comma (,) or semicolon (;).
Format: <Integration_service_hostname>:<port>
Default port: 29436

9. On the **Agent Initiated Monitoring (AIM)** page, you have the option to install the Agent Initiated Monitoring options. Do one of the following:
 - Install one or more of the Agent Initiated Monitoring options:
 - Select **Install Agent Initiated Monitoring** to enable an agent to initiate and stop the recording of a call from the agent's desktop.



The Automated Log On/Off option is *not* supported.

- Select **Enable Block Monitoring** to allow an agent to block the monitoring of call and screen capture sessions that the agent initiates.
- Select **Enable Pause and Resume Monitoring** to allow an agent to pause the recording of both voice and screen activity and then resume recording at a later point in the call.

This feature is useful for preventing the recording of sensitive information while keeping a record of the call itself.

Then click **Next**.

If you do not want to install the Agent Initiated Monitoring options, clear the check marks from all four options on this page, and click **Next**. Skip to Step 11.

10. In the **AIM Annotation Setup** page, if you do not want to enable annotation for AIM, clear the check mark from the **Enable annotation for Agent Initiated Monitors** option and click **Next**. Skip to Step 11. Otherwise, do the following:
 - a. Select **Enable annotation for Agent Initiated Monitors** to enable annotation for AIM.
 - b. In each required **User Field**, type a value.

Values must exactly match what is configured for the Custom Attributes in the Enterprise Manager on the cloud. You do not have to enter a value in all five User Field boxes.
 - c. Select **Define User Tips** to configure a tooltip for each annotation field.

The user tip text is entirely at your discretion. This text should explain to the agent the specific reason each User Field is available for annotation.
 - d. Select **Clear Annotation Field Values** to determine the behavior of the Annotate Call dialog box in the AIM program.

Agents can use the Annotate Call dialog box to enter different annotations for each call. If you select this option, all of the fields on the Annotate Call dialog box are empty each time an agent opens the Annotate Call dialog box.

If you clear this option, the Annotate Call dialog box preserves the settings from the previous time it was used. When an agent opens the Annotate Call dialog box, the dialog box contains the same values that the agent entered the last time the agent used the Annotate Call dialog. This option is useful if agents frequently enter the same annotation information for many different calls.
 - e. Click **Next**.
11. Click **Install**.
12. After the installation is complete, reboot the Desktop. If using Citrix, restart the server to apply changes to all workstations on the server.

Related topics[Configure workstations in TLS environment \(page 28\)](#)**Related information***Security Configuration Guide*

Configure Screen Capture and AIM in a Citrix environment

Perform the instructions in this section if you have installed the Screen Capture Module in a Citrix environment.

i If you have a Citrix desktop environment that does not use Terminal Services, skip the instructions in this section. This section only applies to Citrix environments using Terminal Services with Published Applications.

Use the procedure to identify the Published Applications used by agents in a terminal services environment on Citrix. You must identify Published Applications to prevent the Screen Capture Module from ending prematurely.

Procedure

1. Open the Microsoft Registry Editor.
2. Go to the following key:
HKLM\SOFTWARE\Witness Systems\eQualityAgent\Capture\CurrentVersion
3. Make sure the name and values listed below exist:
 - **Name:** TermSvr
 - **Type:** REG_DWORD
 - **Data:** 1
4. Go to the following key:
HKLM\SOFTWARE\Witness Systems\eQualityAgent\Capture\CurrentVersion\AdditionalUserApps
5. If you do not see AdditionalUserApps, add the key.
6. Add a string value (REG_SZ) to the key for each Published Application (the AimTray.exe application supports screen recording). Ensure that you observe the following restrictions:
 - **Name:** The name should be App1.
 - **Type:** REG_SZ
 - **Data:** The value must match the name of the Published Application executable that is intended to be captured. For example, for Chrome, add "chrome.exe". Do not include the executable's path.

If two or more Published Applications are being used and need to be captured, each Published Application is added one at a time. For example,

Name: App1

Type: REG_SZ

Data: iexplore.exe

Name: App2

Type: REG_SZ

Data: notepad.exe



If a Published Application does not need to be captured, you do not need to add a string value for that Published Application.

Configure Screen Capture and AIM in a VMware Horizon environment

The Capture Service reads the registry for the `ActiveUserDetectionMethod` entry. To generate logon/logoff events for the Recorder Integration Service, this entry identifies how the Capture Service detects currently active user accounts.

Procedure

1. Open the Microsoft Registry Editor.
2. Go to the following key:
`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Witness Systems\eQuality Agent\Capture\CurrentVersion\`
3. If not already there, add the DWORD value named **ActiveUserDetectionMethod**.
4. For a VMware Horizon environment, it is recommended that you set the value to 1.

Related topics

[Screen Capture registry values \(page 139\)](#)

Screen Capture and AIM post installation notes

When installing the Screen Capture Module to work with a Recorder server, the Recorder server must be configured to support screen recording.

To support screen recording, contact your service representative.

Values supported by the Avaya Contact Recorder

The Avaya Contact Recorder only supports the default values:

- Capture Quality 5
- Color Reduction 1
- Compression Quality 1

Screen Capture and AIM silent install parameters

These mandatory and configurable parameters are for silently installing Screen Capture and AIM.

- [Screen Capture basic install parameters \(page 104\)](#)
- [AIM silent install parameters \(page 107\)](#)
- [Terminal Services Server silent install parameters \(page 110\)](#)

Related topics

Refer to [Installation by role: silent distribution \(page 36\)](#) for a sample script that includes the command line for distributing this application in silent mode.

Screen Capture basic install parameters

The properties determine how Screen Capture is configured silently on the agent desktops.

Basic Parameters	Description and Default Values
INSTALLDIR	Installation destination location. Default = <Program Files>\<Company Name>\Screen Capture Module Note: If Selective Screen Application Recording will be used, install the Screen Capture Agent software in \Program Files (x86).
ENCRYPTION_ DATAENCRYPT	Data encryption in-transit selection. Mandatory for cloud. TRUE = data encryption is selected. FALSE = data encryption is not selected. Default=NULL (FALSE).
ENCRYPTION_ WSSPATH	Path for the agent.wss file. Must be a valid Windows path. Default: same path as INSTALLDIR
AGENT_ MONITORING_ ENABLED	Install AIM. TRUE = Install AIM. FALSE = Do not install AIM. Default=NULL (FALSE). Any value other than TRUE, including nothing (NULL), equals FALSE. When true, also use the Screen Capture and AIM silent install parameters (page 104)

Basic Parameters	Description and Default Values
COLOR_REDUCTION	<p>Color reduction.</p> <p>Default=1 for new installations.</p> <p>For upgrades, installation of Screen Capture retain the existing ColorReduction value.</p>
CONN_INTG_SVC	<p>Connection to the Integration Services.</p> <p>TRUE = connection to the Integration Services is selected. Required in agent free-seating environments, or if using legacy non reversal agent recording.</p> <p>FALSE = connection to Integration Services is not selected.</p> <p>Default = NULL (FALSE)</p> <p>NOTE: INTG_SERVERS is enabled when CONN_INTG_SVC=TRUE</p>
INTG_SERVERS	<p>Relevant in agent free-seating environments.</p> <p>When CONN_INTG_SVC = FALSE, set parameter to an empty string.</p> <p>When CONN_INTG_SVC = TRUE, enter a string of comma or semicolon-delimited <server name>:<port number> pairs.</p> <p>Required if using legacy non reversal agent recording.</p>
WDLS	<p>Enable/disables SDK logging.</p>
FQDN	<p>Specifies whether or not the "Send FQDN" parameter is selected.</p> <p>TRUE = select "Send FQDN" parameter.</p> <p>FALSE = do not select the "Send FQDN" parameter.</p> <p>Required if the customer requires FQDN to be sent based on their environment.</p>
SENDFQDN	<p>Set this value to 1 to send the full host name, including the domain.</p> <p>Set this value to 0 to send just the host name.</p> <p>1=Enable</p> <p>0=Disable</p> <p>Default = 0</p> <p>Required if the customer requires FQDN to be sent based on their environment.</p>

Basic Parameters	Description and Default Values
CONN_INTG_CLD	<p>Determines if the Capture Service on the desktop will connect to the Integration Service using the secure cloud protocol.</p> <p>TRUE = connect to Integration Services cloud is selected.</p> <p>FALSE = connect to Integration Services cloud is not selected.</p> <p>Default = NULL (FALSE)</p> <p>INTG_CLOUD is enabled when CONN_INTG_CLD = TRUE</p> <p>Required if customer is using reverse connection secure (SSL) agent recording.</p>
INTG_CLOUD	<p>Enter the host name and port number of the Integration Service that the desktop will connect to using the non-secure cloud protocol. A maximum of eight (8) servers can be added. Separate entries with a comma (,) or semicolon (;).</p> <p>When CONN_INTG_CLD = FALSE, set parameter to an empty string.</p> <p>When CONN_INTG_CLD = TRUE, enter string of comma delimited <server name>:<port number> pairs.</p> <p>Default = ISServer:29435</p> <p>Required if customer is using reverse connection agent recording in a non secure (non SSL) mode.</p>
CONN_SEC_INTG_CLD	<p>Determines if the Capture Service on the desktop will connect to the Integration Service using the secure cloud protocol.</p> <p>TRUE = connect to secure Integration Services cloud is selected. Required in agent free-seating environments.</p> <p>FALSE = connect to secure Integration Services cloud is not selected.</p> <p>Default = NULL (FALSE)</p> <p>SEC_INTG_CLOUD is enabled when CONN_SEC_INTG_CLD = TRUE</p> <p>Required if the customer is using reverse connection secure (SSL) agent recording.</p>
SEC_INTG_CLOUD	<p>Enter the host name and port number of the Integration Service that the desktop will connect to using the secure cloud protocol. A maximum of eight (8) servers can be added. Separate entries with a comma (,) or semicolon (;).</p> <p>When CONN_SEC_INTG_CLD = FALSE, set parameter to an empty string.</p> <p>When CONN_SEC_INTG_CLD = TRUE, enter string of comma delimited <server name>:<port number> pairs.</p> <p>Default = ISServer:29436</p> <p>Required if customer is using reverse connection agent recording in a secure mode (SSL).</p>

Basic Parameters	Description and Default Values
VALUE_SERVER_ENABLED	<p>Used to enable or disable the local web server.</p> <ul style="list-style-type: none"> • 1 - Enabled • 0 - Disabled <p>Note: The VALUE_SERVER_ENABLED, VALUE_MAX_CLIENT, VALUE_SERVER_PORT, and VALUE_REQUIRE_AUTHENTICATION parameters are used to create entries in the desktop registry.</p>
VALUE_MAX_CLIENT	Maximum number of clients allowed to connect to the localhost web server.
VALUE_SERVER_PORT	Listen port for the localhost web server. Valid port range: 1–65535
VALUE_REQUIRE_AUTHENTICATION	<p>Used to enable or disable enforcement of the authorization header on connecting clients.</p> <ul style="list-style-type: none"> • 1 - Enabled • 0 - Disabled

Related topics

[Screen Capture registry values \(page 139\)](#)

AIM silent install parameters

The properties determine how AIM, Manual AIM, AIM Annotation are configured silently on the agent desktops.

Use these parameters when you have enabled AIM installation using the AGENT_MONITORING_ENABLED = TRUE command.

AIM Parameters	Description and Default Values
CTI_BUTTON_GRP	<p>Indicates whether the site uses CTI for recording.</p> <p>CTI = Use CTI for recording.</p> <p>MANUAL = Do not use CTI for recording.</p> <p>Default = CTI</p> <p>Required</p>

AIM Parameters	Description and Default Values
CONNECT_ADPTR_URL	<p>The server name and port number on which the Quality Monitoring Connect Adapter listens for requests.</p> <p>Syntax: CONNECT_ADPTR_URL="<servername>:<port>"</p> <p>Port range: 0 - 65535</p> <p>Default = Witness:3020</p> <p>Required if using Quality Monitoring 6.x and above.</p>
MONITOR_BLOCK	<p>Determines if agents have the ability to block capture sessions they initiate.</p> <p>TRUE = agents enabled to block monitoring they initiate.</p> <p>FALSE = agents not able to block monitoring they initiate.</p> <p>Default: NULL (FALSE)</p> <p>Required</p>
ENABLE_ANNOT	<p>Determines if agents have the ability to annotate captured sessions.</p> <p>TRUE = agents can annotate sessions they initiate.</p> <p>FALSE = agents cannot annotate sessions they initiate.</p> <p>Default = NULL (FALSE)</p> <p>Required</p>
PAUSE_RESUME_MONITOR_VALUE	<p>The silent install inserts the DWORD value 'HKLM\SOFTWARE\Witness Systems\AIM\ PauseMonitoring' into the Registry.</p> <p>Determines if agents have the ability to pause and resume monitoring a call for security and confidential card information reasons.</p> <p>1 = agents can pause and resume contact recording.</p> <p>0 = agents cannot pause and resume contact recording, and cannot view the Pause Monitoring and Resume Monitoring AIM menu options.</p> <p>Any valid Windows path.</p> <p>Default: 0</p> <p>Required</p>
AGENT_LOGS	<p>Specifies the drive and path used by AIM to store and write log files.</p> <p>Any valid Windows path.</p> <p>Default: <Program Files>\Witness Systems\Screen Capture Module\Logs</p> <p>Required</p>

Manual AIM Parameters	Description and Default Values
AGENT_EXTENSION	Use to automatically populate agent extension when they log on to AIM. Number. Default: 1234 Required
AGENT_EXTENSION_LOCK	Determines if agents can change their extensions when logging on to AIM. 1 = agents cannot change extensions when logging on. 0 = agents can change extensions when logging on. If you do not want to lock extensions, exclude this parameter. Default: 0 Required
AGENT_ID	Use to automatically populate agent ID when an agent logs on to AIM. Number Default: 1234 Required
AGENT_ID_LOCK	Determines if agents can change their Agent IDs when logging on to AIM. 1 = agents cannot change IDs when logging on. 0 = agents can change IDs when logging on. If you do not want to lock extensions, exclude this property from the command line. Default: 0 Required
AIM Annotation Parameters	Description and Default Values
You must map these annotation properties to attributes using the Enterprise Manager on the cloud. Annotations are considered customized attributes. For details, see the <i>Recorder Configuration and Administration Guide</i> .	

AIM Annotation Parameters	Description and Default Values
ANNOT_USER	<p>Determines the user fields available for annotation. These fields must also be configured in the database, and configured in Quality Monitoring.</p> <p>Syntax: ANNOT_USER<n>="UserField<n>"</p> <p>(where <n> is an integer from 1 to 5)</p> <p>String</p> <p>Default: UserFieldn.</p> <p>You do not have to provide values for all five fields.</p>
USERTIP	<p>Determines the user tips available for annotation.</p> <p>Syntax: USERTIP<n>="<value n>"</p> <p>(where n is an integer from 1 to 5)</p> <p>String</p> <p>Default: This is User Field n.</p> <p>You do not have to provide values for all five fields.</p>

Terminal Services Server silent install parameters

The parameters in the Screen Capture and AIM Parameters for Terminal Services Servers table are applicable only for deployments with a Quality Monitoring package.

Screen Capture and AIM Parameters for Terminal Services Servers	Description and Default Values
AIM_TERMINAL_SERVICES	<p>Determines whether anonymous terminal logon with screen only workspaces should be enabled.</p> <p>1 = TRUE</p> <p>0 = FALSE</p> <p>Any value other than 1, including nothing (NULL), equals 0 (FALSE).</p> <p>Only available for Quality Monitoring 6.x and above.</p> <p>Default: 0 (FALSE)</p> <p>Required</p>
WS_TERMINAL_SERVER_LIST	<p>BDR Server Name and Port Number for the Terminal Services Adapter in the format: <ServerName:Port></p> <p>Only available for Quality Monitoring 6.x.</p> <p>Default: Witness:3022</p> <p>Required</p>

Screen Capture and AIM Parameters for Terminal Services Servers	Description and Default Values
WS_TERM_SERVER_AGENTID	<p>Choose from either the Named Terminal Services Terminal or the Anonymous Terminal Services Terminal.</p> <p>0 (Named Terminal Services Terminal -Thin client terminals have hostnames assigned to them)</p> <p>1 (Anonymous Terminal Services Terminal - Thin client sessions is identified using the Windows username of the user)</p> <p>Default: 0 (Named Terminal Services Terminal)</p> <p>Required</p>

Strategic Planner Client

Strategic Planner allows you to plan long term for multi-skilled contact center and enterprise back-office environments.

Strategic Planner can also be used to:

- assess operational and financial benefits
- assess impact of different scenarios before making decisions
- increase forecasting accuracy with sophisticated analysis of historical data
- plan your resources to reflect projected customer demand and corporate objectives
- develop optimal staffing plans that minimize costs while meeting service goals
- provide executives with the information they need to review and rapidly approve budgets and plans

Related topics

[Customer requirements \(page 19\).](#)

Install Strategic Planner manually

Manually install the Strategic Planner using the Setup msi.



To import and export data from other WFM applications, Strategic Planner users must logon with the Application Load Balancer address. Users can set the Application Load Balancer address in the Configuration screen during the installation.

The Application Load Balancer address can be updated after the installation process. To modify the address, after the initial installation, go to **C:\Users\[INTUSERNAME]\StrategicPlanner**. In the **src** subfolder of the installation location, open the appProperties file with a text editor and modify the appserver name manually in this file.

For import and export data into the database, the user must have the following privileges:

- View Organization
- View Queues

Before you begin

- Download the Strategic Planner installation package, according to [Obtain the installation packages \(page 18\)](#).



To ensure that you have the latest software, get the installation packages from the portal or from your customer representative.

Procedure

1. To start the Installation Wizard, do one of the following:
 - (recommended) If downloaded from the portal, double-click the KB<number>.msi file.
 - OR
 - If installing from the media, double-click **StrategicPlannerSetup.msi**.
2. On the **Welcome** page, click **Next**.
3. On the **End-User License Agreement** page, select **I accept the terms in the license agreement**, and then click **Next**.
4. On the **Choose Destination Location** page, click **Next** to install to the default folder, or click **Change** to install to a different folder.
5. On the **Configuration** page, enter the Application Load Balancer address , followed by the **Port Number**.
 - a. If you want to use a separate authentication server, such as IdP, click the check box next to **Do you need to use a separate authentication server?**
 - b. Click **Next**.
6. On the **Install Confirmation** page, click **Install**.
7. When the installation is complete, the **Installation Success** page appears. Click **Finish**.

Configure the license key for Desktops

Upon accessing the Strategic Planner for the first time on the Desktop, you must enter the company name and license information.

Procedure

1. Open the Strategic Planner for the first time.
A pop-up window opens requesting company and license information.
2. Type the information about the company name and the license key.

Related topics

[Configure the license key for Citrix \(page 113\)](#)

Configure the license key for Citrix

For Citrix installations, the system administrator can (optionally) configure it so that multiple users are not each prompted to enter a license code.

Procedure

1. In the following folder, create a **ltp_args_override.cmd** file:
C:\Program Files (x86)\Verint\Strategic Planner\src folder

- Using a text editor, open the file and add the following:
set LTP_jvm_args="-DLicense.LicenseText=<License>" "-DLicense.CompanyName=<Company>"
where:
<License> = Valid license
<Company> = Name of the company to which the license is issued
- Optional. You can also add other items (such as AppServer) on the same line separated by a space.
For example: **"-DAppServer=<Server Url>"**
- Save the file and start the Strategic Planner application.

Related topics

[Configure the license key for Desktops \(page 113\)](#)

Strategic Planner silent install parameters

The properties determine how Strategic Planner is silently configured.

Parameters	Description and Default Values
MsiFile	Installation file name: StrategicPlannerSetup.msi
/qn	Silent mode switch. Mandatory
SZAPPSERVERNAME	Application Load Balancer address
SZAPPSERVERPORT	Port number of the Application Load Balancer

Related topics

For a sample script that includes the command line for distributing this application in silent mode, see [Installation by role: silent distribution \(page 36\)](#).

Face to Face Voice Interaction Recording

For Face to Face Voice Interaction Recording, see the *Face to Face Voice Interaction Recording Installation and Configuration Guide*.

Related information

Face to Face Voice Interaction Recording Installation and Configuration Guide

Advanced administration for desktop applications

System administration for desktop applications includes tasks that are not necessarily part of the initial installation, but are tasks you might need to perform due to changes in the cloud.

Topics

Application configuration updates 117

Application configuration updates

It is required to update the Desktop Applications' configuration files in the following cases:

- [Modifying desktop computer name \(page 117\)](#)
- [Application Load Balancer name change \(page 117\)](#)
- [Update desktop application configuration files \(page 118\)](#)

Modifying desktop computer name

If you intend to rename the computer name of the desktop, remove MSMQ from the computer before renaming the computer. Then, reinstall MSMQ.

The reason is that MSMQ tries to create the msmqConfiguration object with the globally unique identifier (GUID). However, msmqConfiguration is already using this GUID under the old computer object.

Application Load Balancer name change

There are Desktop Applications that rely on communication with the Application Load Balancer (ALB). When a change is made, a corresponding change to the Desktop Applications configuration is required.

When name changes can occur?

- Application Load Balancer (ALB) name change
- IT policy computer name changes
- Expansion scenarios
- Changing default SAML SP-initiated sign-in to IdP-initiated sign-in

Face to Face Voice Interaction Recording

If the Data Center Server Host Name changes, do the following to update the desktop:

1. Reinstall the Face to Face Voice Interaction Recorder using the new data center host details.
2. If you are using Configuration Publisher, change the data center host server name following the "Manage System Configuration" section in the Face to Face Voice Interaction Recorder documentation.
3. Push the new configuration to the application server.

Related topics

[Update desktop application configuration files \(page 118\)](#)

Related information

Face to Face Voice Interaction Recorder Installation and Configuration Guide

Update desktop application configuration files

This section details the configuration files that require update.

Related topics

[Playback configuration \(page 118\)](#)

[Form Designer configuration \(page 119\)](#)

[Desktop and Processing Analytics \(DPA\) configuration \(page 120\)](#)

[Desktop Messaging configuration \(page 120\)](#)

[Strategic Planner configuration \(page 120\)](#)

Playback configuration

ProxyWebService

- Key: ProxyWebService
 - Path:
 - 32-bit system: HKEY_LOCAL_MACHINE\SOFTWARE \<Company Name>\CryptoSDK
 - 64-bit system: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\<Company Name>\CryptoSDK
 - Default value (string): 1
 - Required update for TLS: No
- The Application Load Balancer name must match the name of the certificate on the Application Load Balancer.

isSSL

- Key: isSSL
 - Path:
 - 32-bit system: HKEY_LOCAL_MACHINE\SOFTWARE \<Company Name>\CryptoSDK
 - 64-bit system: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\<Company Name>\CryptoSDK
 - Default value (string): https://<server or LB name>/KeyProxy/ManagementService.asmx
 - Required update for TLS: No.
- For non-TLS the required value is 0.

AuthPort

- Key: AuthPort
- Path:
 - 32-bit system: HKEY_LOCAL_MACHINE\SOFTWARE \<Company Name>\CryptoSDK
 - 64-bit system: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\<Company Name>\CryptoSDK
- Default value (string): 7002

- Required update for TLS: No
This key is used only when playing calls from a system prior to V11.2.

Form Designer configuration

FormManagementWS

- Key:
Verint.EvaluationPackage.FormManagement.FormManagementControlLibrary.FormManagementWS.FormManagementWS
- Path: <Software Drive>\Program Files\<Company Name>\FormDesigner\Verint.EvaluationPackage.FormManagement.FormManagementUI.exe.config
- Default value (string): http://<Application Load Balancer address>/FormManagementWS/FormManagementWs.asmx
- Required update for TLS: No

HTTPS

- Key:
Verint.EvaluationPackage.FormManagement.FormManagementControlLibrary.FormManagementWS.S.FormManagementWS.HTTPS
- Path: Not applicable
- Default value (string): https://<Application Load Balancer address>/FormManagementWS/FormManagementWs.asmx
- Required update for TLS: No

FilloutPathForPreview

- Key: FilloutPathForPreview
- Path: Not applicable
- Default value (string): http://<Application Load Balancer address>/Fillout/EvaluationForm.aspx
- Required update for TLS: Yes

AuthUrl

- Key: AuthUrl
- Path: Not applicable
- Default value (string): http://<Application Load Balancer address>/wfo/control/signin?screen=QM_ACTIVEX_LANDING_PAGE&integrationURL=magic
If you change to SAML IdP-initiated sign-in, **AuthUrl** must be according to the service provider's specifications.
- Required update for TLS: Yes

Desktop and Processing Analytics (DPA) configuration

If the server hosting the DPA server roles has a new name, you must update the clients to point to the new server.

1. Reinstall the DPA clients with new server details.

Desktop Messaging configuration

When the server domain or name has changed, do the following to update the desktop.

1. Reinstall the Desktop Connection Manager client with new server details.

DPA Process Discovery configuration

If the Process Discovery service is hosted on the new DPA server, for example in a gradual upgrade scenario, update the **WebService URL** setting with the address of the Process Discovery service hosted on the new DPA server.

Related information

Generate Process Discovery Diagrams (*Desktop and Process Analytics (DPA) User Guide*)

Strategic Planner configuration

If the Application Load Balancer has a new address, for example in a gradual upgrade scenario, update the Strategic Planner clients with the new Application Load Balancer address as a secondary server.

Procedure

1. Open with a text editor the **appProperties** file, located in **C:\Users\[NTUSERNAME]\StrategicPlanner**.
2. In the **AuthServer** property, set the new Application Load Balancer address as the secondary address. If you change to SAML IdP-initiated sign-in, **AuthUrl** must be according to the service provider specifications.
3. In the **AppServer** property, keep the primary Application Load Balancer address.
4. To use SSO, set the UseSSO property to True.

Example URL to be added in the appProperties file:

```
AppServer=https://wfo.cloudservername.verintcloudservices.com/  
AuthServer=https://adfs.wfo.verintcloudservices.com/adfs/ls/idpinitiatedsignon.aspx
```

In the above example, AppServer value is set to the Primary Application URL. AuthServer is set to the Idp-initiated-sign-in URL.

Proxy configuration

- Open file location of the Strategic Planner desktop shortcut, it will go to the file “C:\Program Files (x86)\Verint\Strategic Planner\src\ltp.cmd”
- Open the file in a text editor
- Go to line 87, it should contain the following code:

```
set LTP_jvm_opts_1=%LTP_mem_args% -XX:+HeapDumpOnOutOfMemoryError -  
XX:HeapDumpPath=%LOGS_DIR% -DLOGS_DIR=%LOGS_DIR% -Djavax.net.debug=all -  
Djava.library.path=%LIB_PATH% %net_options%
```

- At the end of the line add the two following parameters:

1. For HTTP connection:

```
Dhttp.proxyHost=server, example: -Dhttp.proxyHost=example.com  
Dhttp.proxyPort=port, example: -Dhttp.proxyPort=8080
```

2. For HTTPS connection:

```
Dhttps.proxyHost=server, example: -Dhttps.proxyHost=example.com  
Dhttps.proxyPort=port, example: -Dhttps.proxyPort=8080
```

- You can try also including both types of connections HTTP and HTTPS with specifying all the four above parameters
- If there is authentication, also add:

```
Dhttps.proxyUser=user  
Dhttps.proxyPassword=password
```

Example: Examples of the modified line

 Items in **bold** should be replaced with customer-specific values.

- HTTP

```
set LTP_jvm_opts_1=%LTP_mem_args%  
-XX:+HeapDumpOnOutOfMemoryError  
-XX:HeapDumpPath=%LOGS_DIR%
```

```
-DLOGS_DIR=%LOGS_DIR% -Djavax.net.debug=all  
-Djava.library.path=%LIB_PATH% %net_options%  
-Dhttp.proxyHost=example.com -Dhttp.proxyPort=8080
```

- **HTTPS**

```
set LTP_jvm_opts_1=%LTP_mem_args%  
-XX:+HeapDumpOnOutOfMemoryError  
-XX:HeapDumpPath=%LOGS_DIR% -DLOGS_DIR=%LOGS_DIR%  
-Djavax.net.debug=all  
-Djava.library.path=%LIB_PATH% %net_options%  
-Dhttp.proxyHost=example.com  
-Dhttp.proxyPort=8080
```

- **HTTP and HTTPS**

```
set LTP_jvm_opts_1=%LTP_mem_args%  
-XX:+HeapDumpOnOutOfMemoryError  
-XX:HeapDumpPath=%LOGS_DIR%  
-DLOGS_DIR=%LOGS_DIR%  
-Djavax.net.debug=all  
-Djava.library.path=%LIB_PATH% %net_options%  
-Dhttp.proxyHost=example.com  
-Dhttp.proxyPort=8080  
-Dhttps.proxyHost=example.com  
-Dhttps.proxyPort=8080
```

- **HTTP and authentication**

```
set LTP_jvm_opts_1=%LTP_mem_args%  
-XX:+HeapDumpOnOutOfMemoryError  
-XX:HeapDumpPath=%LOGS_DIR%  
-DLOGS_DIR=%LOGS_DIR%  
-Djavax.net.debug=all  
-Djava.library.path=%LIB_PATH% %net_options%  
-Dhttp.proxyHost=example.com  
-Dhttp.proxyPort=8080  
-Dhttps.proxyUser=user  
-Dhttps.proxyPassword=password
```

- **HTTP, HTTPS and authentication**

```
set LTP_jvm_opts_1=%LTP_mem_args%
-XX:+HeapDumpOnOutOfMemoryError
-XX:HeapDumpPath=%LOGS_DIR%
-DLOGS_DIR=%LOGS_DIR% -Djavax.net.debug=all
-Djava.library.path=%LIB_PATH% %net_options%
-Dhttp.proxyHost=example.com
-Dhttp.proxyPort=8080
-Dhttps.proxyUser=user
-Dhttps.proxyPassword=password
-Dhttps.proxyUser=user
-Dhttps.proxyPassword=password
```

Phonetic Boosting configuration

WfoRelativeUrl

- Key: WfoRelativeUrl
- Path: <Software Drive>\Program Files\<Company Name>\Phonetics Boosting Application\PhoneticsBoosting.exe.config
- Default value (string): /wfo/control/signin?screen=QM_ACTIVEX_LANDING_PAGE&integrationURL=magic

AlternativeLoginUrl

- Key: AlternativeLoginUrl
- Path: <Software Drive>\Program Files\<Company Name>\Phonetics Boosting Application\PhoneticsBoosting.exe.config
- Default value (string): For SP-initiated sign-in, **AlternativeLoginUrl** must be the WFO address. If you change to SAML IdP-initiated sign-in, **AlternativeLoginUrl** must be according to the service provider's specifications.

Upgrade legacy desktop applications

This chapter outlines the procedures required to upgrade the desktop applications from previous versions.

Topics

Upgrade V15.1 workstations	125
DPA client upgrade	128
Transition to TLS	129

Upgrade V15.1 workstations

The customer is responsible for upgrading the desktop applications.

For V15.1 desktop applications that are compatible with V15.2, you can leave the V15.1 desktop application and upgrade after the migration to Avaya Experience Platform™ Workforce Engagement (cloud) as per the following table.

For V15.1 desktop applications that are not compatible with V15.2, you must upgrade these applications before connecting to the cloud.

Desktop applications upgrade instructions from V15.1

Desktop application	Upgrade instructions
Desktop Resources	Pre-requisite package. Install V15.2 to replace previous version.
Logger	Upgrade to V15.2 before the migration.
Plugin Player	After upgrading Windows, you must uninstall and then reinstall the Plugin Player.
Strategic Planner	Upgrade to V15.2 before the migration.
Screen Capture Module and AIM	When upgrading, uninstall is not required. Upgrade the Screen Capture module in the following order: <ol style="list-style-type: none"> 1. Upgrade to V15.2 HFR7 190XXX series of KBs. 2. Upgrade to 2020R1 200XXX series of KBs.
Desktop and Process Analytics (DPA) Client	DPA client in-place upgrade (V15.1 to latest): You can install any latest DPA client without uninstalling the V15.1 client. There is a single entry in add remove programs after latest DPA client is installed. This upgrade does not support rollback or repair to previous version.
DPA Process Discovery	Upgrade to V15.2 before the migration.
Form Designer	Upgrade to V15.2 before the migration.
Desktop Messaging	Upgrade to V15.2 before the migration.
Desktop Gadgets	Remove. No longer supported.

To upgrade a desktop application:

1. Ensure all customer requirements are met for V15.2 desktop applications.
2. Download the most up-to-date installation package from the Latest Hotfixes area of the Online for Customer's site.
3. Install the V15.2 desktop resources pre-requisite package (replaces the previous version).
4. Uninstall the V15.1 desktop application except the Screen Capture and AIM.
5. Install the V15.2 desktop application.
6. Once the Data Center migration completes, configure the relevant Desktop Applications to point to the V15.2 Application Load Balancer (see *Application Configuration Updates*).

Related topics[Customer requirements \(page 19\)](#)[Silent uninstall \(page 126\)](#)[Obtain the installation packages \(page 18\)](#)[Installation by role: silent distribution \(page 36\)](#) (refer to the relevant desktop application)[Installation by application \(page 46\)](#) (refer to the relevant desktop application)[Application configuration updates \(page 117\)](#)

Silent uninstall

It is possible to remove desktop applications silently even if you do not have the original MSI file that was used for the installation. Each MSI file contains a product code (GUID) regardless of its version. You use this GUID in the command **msiexec.exe /x {GUID}**.

Procedure

1. Identify the display name and GUID of the desktop component to uninstall as follows:
 1. From **Windows Control Panel > Programs and Features**, identify the display name of the desktop component.
 2. Open the registry (run regedit).
 3. For 32-bit system, search for the component display name in:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
 4. For 64-bit system, search for the component display name in:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
 5. Note the GUID of the desktop component.
2. Run the following command line with the specific GUID of the desktop application:
msiexec.exe /x {GUID} /qn

3. To create a log file during the removal, add to the end of the command line:

```
/l*v <drive:\folder\log_name.log>
```

Example:

To remove the playback application and create a log, run the following command (including the braces):

```
msiexec.exe /x {47B60717-B543-437A-B398-2684F7A16F16} /qn /l*v C:\logs\playback_uninstall.log
```

DPA client upgrade

The DPA client has a legacy V11.1 version, and a newer, platform agnostic version, version V15.x. The latest release of the DPA client is cross-compatible with all server versions from V11.2, V15.1, and V15.2 onwards.

Install multiple DPA clients side-by-side

The V11.x and V15.x versions of the DPA client can be installed side by side for a short period of time, typically the one to two weeks required for a switchover. Only V11.x and V15.x can be installed side by side. The V15.1 and V15.2 clients cannot coexist.

- Clients are identified by a version number (first three digits), and a revision number.
- Uninstall a newer version of the DPA client, before installing an older version.
- Installing a newer version while the existing version is active will prompt a restart.
- Rollback to an older client version includes removing the newer version, and then repairing the target version. This is likely to require a restart of the operating system.

DPA client maintenance

Removal or clean-up of older V11.2 – V15.x DPA client versions is not recommended. If required, the currently active installed version must be repaired after uninstall of any newer V11.2 – V15.x version when reverting that newer version.

V11.0 and V11.1 client versions are considered legacy and must be removed when a V11.2 – V15.x client is deployed without exception.

Transition to TLS

When moving to Avaya Experience Platform™ Workforce Engagement, it is required to update desktop applications configuration to support TLS communication.

Related topics

[Update desktop application configuration files \(page 118\).](#)

[Configure workstations in TLS environment \(page 28\)](#)

Screen Capture module and AIM

To ensure you can install and configure the application to operate successfully in your environment, this appendix includes additional information about the Screen Capture Module software. Review this information before installing the Screen Capture Module.

Topics

Introduction to the Screen Capture module and AIM	131
Installation in a Citrix or Terminal Services environment	132
Installation on Azure Virtual Desktop	136
Installation in an Amazon WorkSpace environment	137
Screen Capture and AIM registry settings	139
Configuration required to support AIM call annotation	167
Enable multi-monitor Screen Capture support	174
Encrypt screen recordings in-transit	176
Use a proxy server for screen capture	177
Screen capture proxy for live monitoring on Chrome configuration	178
Known issues for the Screen Capture module	179
CapTestB utility	185

Introduction to the Screen Capture module and AIM

You can install the Screen Capture Module to work with the Recorder server and the Quality Monitoring Application. For Screen Capture Module installations instructions, see [Screen Capture and AIM \(page 99\)](#).

Topics

- [Installation in a Citrix or Terminal Services environment \(page 132\)](#) - Explains the unique considerations and configurations associated with installing the Screen Capture Module on a Citrix server or a Terminal Services server. Read this section for performance optimization of Screen Capture Modules installed in a Citrix or Terminal Services environment.
- [Screen Capture and AIM registry settings \(page 139\)](#) - Discusses all the registry settings for the Screen Capture component and the Agent Initiated Monitoring (AIM) component of the Screen Capture Module. Use the registry settings for fine-tuning the performance or to change the application configuration after it is installed.
- [Configuration required to support AIM call annotation \(page 167\)](#) - Explains all configurations you must perform to enable agents to annotate calls from the AIM application.
- [Enable multi-monitor Screen Capture support \(page 174\)](#) - Explains how to record screen images on agent workstations that have multiple monitors.
- [Encrypt screen recordings in-transit \(page 176\)](#) - Provides a reference to Encrypt Screen Recordings In-Transit in the *Security Configuration Guide*.
- [Known issues for the Screen Capture module \(page 179\)](#) - Discusses the known issues with the Screen Capture Module.

Installation in a Citrix or Terminal Services environment

This section discusses special considerations and configurations when installing the Screen Capture Module on a Citrix or Terminal Services server.

Related topics

[Supported Terminal Server sessions \(page 132\)](#)

[Limitations and best practices \(page 133\)](#)

[Memory utilization on a Terminal Server \(page 135\)](#)

Supported Terminal Server sessions

Screen Capture is supported for the following types of Terminal Server sessions:

- Anonymous Terminal Session (where remote terminal host name is not available)
- Named Terminal Session (where remote terminal host name is available)

The Recorder supports Agent Initiated Monitoring (AIM) in remote sessions where the notification area is displayed. The AIM icon is available only in the notification area.

Screens captured in a terminal services or Citrix environment are saved in the Recorder server call buffer in the same format as other desktop screen data.

Related topics

[Thin clients and VMware \(page 22\)](#)

Limitations and best practices

Limitations exist for screen capture of multiple sessions and Published Applications in Windows Terminal Services and Citrix environments. This section discusses best practices you can employ to minimize these limitations.

Citrix published applications

The DPA client command can be appended to existing published applications or set when publishing new applications.

There are two separate procedures that you can perform here. Perform one procedure if the published application is launched directly from the command line. Perform a separate procedure if the published application is launched by a script.

Published application launched from the command line

Procedure

1. If the published application is launched directly from the command line, add the following to the command line of each published application:

```
C:\<company_name>\DPA\Client\TsStart.exe <"path to executable">
```

Example:

```
N:\<company_name>\DPA\Client\TsStart.exe  
"C:\WINNT\System32\mspaint.exe"
```

Published application launched by a script

Procedure

1. If the published application is launched by a script, use TsStart within the script as follows:

Example:

```
@Echo off  
SET HOMEDRIVE=%USERPROFILE%  
N:\<company_name>\DPA\Client\TsStart.exe  
"C:\WINNT\System32\mspaint.exe"
```

The TsStart.exe always requires a command line parameter containing the path to the executable to be published. A call that includes TsStart.exe without a command line parameter containing the path to the executable to be published will not execute.

Citrix published applications Screen Capture limitations

In capturing screens for Published Applications, the Recorder server records only one Citrix session at a time per agent.

The capture depends on the type of Citrix session.

If the Citrix Session is:

- A Published Server Desktop session, then it records all activities in that Desktop session.
- An individual Published Application session, then it records only that particular Published Application. In this scenario, you can configure `explore.exe` as the individual Published Application and add shortcuts to other applications in a Windows folder. All applications opened from within this folder run in the `Explorer.exe` session. This configuration allows you to record all activities from multiple applications even though only a single application (`Explorer.exe`) is published. See the [Configuration details \(page 134\)](#) for instructions on configuring `Explorer.exe` as the Published Application.
- A session that is shared between Published Applications, then it records all the Published Applications in that session. You can configure published Applications with common properties (color depth, resolution, encryption, and related properties) to share a session within Citrix. Refer to <http://support.citrix.com/article/CTX159159> for session sharing details.

Capture limitations

- Multiple simultaneous sessions cannot be recorded:

If the agent opens multiple Published Applications (not by session sharing) from a single Citrix Server, then recording of only one session occurs.

If the agent opens multiple Published Applications from different Citrix servers in a Citrix server farm, then recording of only one session occurs.

- The session recorded is the session most recently created.

Example:

The agent first opens Email as a published application on one server.

The agent next opens CRM as an application on a different server.

The CRM application session is recorded and associated with the next call for the agent. If the agent opens CRM first and then Email second, Email is recorded and associated with the next call for the agent.

Configuration details

Enable the recording of all Published Applications when the determination of which screen to record is not predictable:

- Restrict each agent to a single Citrix Server in a Citrix Server Farm at a particular time. Do not allow the agent to connect to multiple Citrix Servers in the Server Farm.
- Record all Applications an agent uses by doing one of the following:

Configure Published Applications so they share a session.

Publish the Server Desktop and allow agents to access all the applications through the Desktop session.

Configure `Explorer.exe` as the Published Application and give one of the folder names as the argument. In that folder, use Windows Explorer to create file shortcuts to applications. When the `Explorer.exe` is launched on the client workstation, it opens the folder containing the shortcuts. Only one session is created on the Citrix Server when the `Explorer.exe` program is launched.

Open applications using the shortcuts available from the folder in Explorer.exe. All applications launched using the shortcuts run in the same Explorer.exe session.

Capture Service and Recorder Integration Service limitations

The capture service can only support a maximum of eight connections to Recorder Integration Services (RIS) or Avaya Contact Recorders.

Deployments with redundant RIS deployments are limited to four pairs of RIS servers. Keep this list to a minimum. Regardless of the stated maximum of eight connections, connecting to RIS servers that do not need logon events can result in:

- Extra load on the unrelated RIS servers.

Each desktop pointed to the unrelated servers still counts as a device and against the sizing maximums of the RIS server in that regard.

- Real Time Monitoring (RTM) failure for associated agents.

RIS servers report known agents to the RTM system. If the capture service is set up to send logins to two RIS systems (one correctly and one unrelated), both can report status to the RTM system. The result is RTM failure. If an employee is associated with an RIS by means of an organization, then it tracks the employee.

Memory utilization on a Terminal Server

Use the specified formula when estimating the capture memory utilization.

Formula

$$M = 2000 + (4 * H * W * D) / 1000$$

Where:

M - memory per user in KB

H - screen height in pixels

W - screen width in pixels

D - color depth in bytes

Installation on Azure Virtual Desktop

Azure Virtual Desktop (AVD) is a virtual Windows desktop hosted in the Azure cloud and accessed using a client, such as Windows, which renders the desktop and shared applications. With the appropriate configuration, the Screen Capture Agent is able to capture AVD desktops.

AVD configuration requirements

- The AVD can be configured in one of two ways:

One VM per user

Multiple users per VM

The Screen Capture module must be installed using administrative privileges. The software is installed once per AVD multi-session host.

- On Windows 10, for the Microsoft desktop duplication technology to correctly capture the AVD desktops, the Virtual Machine (VM) must be configured to use an XDDM display driver. (Windows 11 works correctly with the WDDM graphics display driver.)

To set the display driver, access the Microsoft Windows Group Policy Editor:

1. Go to Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host.
2. Under Remote Session Environment, set the Policy [Use WDDM graphics display driver for Remote Desktop Connections] to Disabled.

- For the AVD multi-session environment to correctly close disconnected sessions, complete the following configuration.

As an administrator, access the Microsoft Windows Group Policy Editor:

1. Go to Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host.
2. Under Session Time Limits, set the Policy [Set time limit for disconnected sessions] to the amount of time in which the disconnected session remains active. The suggested setting is one minute.

Screen capture configuration requirements

If using the default connection mode where the agent capture module connects to the RIS and screen recorder, the virtual desktop must be configured to allow outgoing connections from the agent capture module.

Related topics

[Install Screen Capture and AIM manually \(page 99\)](#)

Installation in an Amazon WorkSpace environment

Amazon WorkSpaces are virtual Windows desktops hosted in the Amazon Web Service (AWS) cloud. WorkSpaces are accessed using a client which renders the Windows desktop and shared applications.

Amazon WorkSpace Users

Each WorkSpace is assigned to one user. More than one user cannot use a WorkSpace. By default, only one WorkSpace per user per directory is allowed.

Amazon WorkSpace Windows Installation

Each Amazon WorkSpace has its own unique Windows 10 installation under the C:\ drive. Screen Capture is installed on each Windows 10 workspace, rather than a terminal server installation.

Screen Capture can be installed manually or using silent distribution.

Amazon WorkSpace Network Ports

Each Amazon WorkSpace has its own unique host name and IP number. Screen Capture is installed and configured as a typical Windows 10 workstation, rather than a terminal server installation.

Amazon WorkSpace operating systems

The Amazon WorkSpace operating system must be 64-bit.

Operating system	Description	Supported
Windows 10 Desktop	Windows 10 Desktop Experience. Powered by Windows Server 2016.	Yes
Amazon Linux	Amazon Linux WorkSpaces built on Amazon Linux 2 LTS	No

Amazon WorkSpace clients

The following table identifies the clients that can be used to access the Remote Desktop and applications.

Client	Workspace protocol	Supported
iPad	PCoIP	Yes*
Mac OS X		Yes**
Windows 32-bit	WSP	Yes*
Windows 64-bit	WSP	Yes*
Android/Chromebook	PCoIP	Yes*

Client	Workspace protocol	Supported
Fire tablet		Yes**
Web Access	PCoIP	Yes*
Amazon Linux	PCoIP	Yes**

* Tested with the default Microsoft Desktop Duplication API (Microsoft DDAPI).

** Has not been verified in a Verint lab.

Screen Capture installation requirements

- Install Screen Capture using an administrative user name and password.
- Each Amazon WorkSpace has its own unique host name and IP number.
- If Selective Screen Application Recording is used, install the Screen Capture Agent software in \Program Files (x86).
- After the Screen Capture software is installed and configured, restart the desktop.
- If using the default connection mode where the agent capture module connects to the RIS and screen recorder, the virtual desktop must be configured to allow outgoing connections from the agent capture module.

Related topics

[Install Screen Capture and AIM manually \(page 99\)](#)

[Installation by role: silent distribution \(page 36\)](#)

[Registry values for Terminal Services support \(page 156\)](#)

Screen Capture and AIM registry settings

You can change the Windows registry settings after installation. Change registry settings to fine-tune the Agent Capture Service or Agent Initiated Monitoring (AIM) performance. You can also enable extra features after installation.

This section provides reference information for all registry keys available for the Agent Capture Service and the Agent Initiated Monitoring (AIM) applications. You can find the registry key locations and the possible values for each key.

Registry key locations

The Screen Capture registry key locations for a 32-bit system, 64-bit system, and AIM registry keys are provided.

32-bit system

[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion]

64-bit system

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\eQuality Agent\Capture\CurrentVersion]

For information on the individual Agent Capture Service registry keys, see [Screen Capture registry values \(page 139\)](#) and [Registry values for Terminal Services support \(page 156\)](#).

AIM registry keys

For 32-bit system: [HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\AIM]

For 64-bit system: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\AIM]

For information on the individual AIM registry keys, see [AIM registry values \(page 156\)](#).



Use caution when changing registry values. Editing the registry incorrectly can result in program instability.

Screen Capture registry values

The Screen Capture registry key locations for a 32-bit system and a 64-bit system are provided.

32-bit system

[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion]

64-bit system

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\eQuality Agent\Capture\CurrentVersion]

Screen Capture executable

The Screen Capture executable name is WcapW32.exe. You can set specific Agent Capture Service entries.

Screen Capture registry values

Registry Entry	Description	Type	Default Value
Active User Detection Method	<p>Add this setting if it is missing in the registry and you want to change the default value. The entry defines how the Capture Service identifies the active user on the workstation. This setting does not apply to terminal servers.</p> <p>If the value is missing, or set to a value other than 1, the Capture Service uses the historical detection method.</p> <p>If set to 1, Capture Service uses the alternative detection method, which is more reliable for later systems.</p>	REG_DWORD	By default, value is missing from NT Registry.
Agent Socket Port	Socket TCP port number to listen on for connection request from the recorder server when the Screen Capture Module is installed on an agent workstation.	REG_DWORD	4001
Capture Layered Windows	<p>Set this value to 1 to capture layered windows, such as transparent windows, tool tips, and related settings. Setting this value to "1" increases the Screen Capture software CPU utilization.</p> <p>To capture screens using newer versions of the Avaya One-X Agent, set CaptureLayeredWindows to 1.</p> <p>0 - Disabled 1 - Enabled</p>	REG_DWORD	0
Capture Quality	Can be changed from 1 to 10, where 10 indicates the highest quality. Increasing the setting results in higher CPU utilization.	REG_DWORD	7
CaptureRun Path	Agent Capture installed directory path.	REG_SZ	""

Registry Entry	Description	Type	Default Value
Cloud Integration Services Server List	<p>Comma-delimited or semicolon-delimited list of Integration Services server names and ports that the Capture Service uses to connect using a <i>non-secure</i> protocol. The Capture Service only connects to the first eight (8) hosts within the list.</p> <p>This setting controls how Screen Capture connects to the Recorder Integration Service and is applicable to both on-premise and cloud environments.</p> <p>Screen Capture supports automatic migration to this connection protocol and populates this setting with servers from the "Integration Services Server List" registry entry that supports the new interface.</p> <p>A given server should exist in either the "Cloud Integration Services Server List" or the "Secure Cloud Integration Services Server List", but not both. A server may continue to have an entry in the "Integration Services Server List" for fallback connectivity.</p> <p>Example: hostname1:port1,hostname2:port2</p>	REG_SZ	""
Color Reduction	<p>Reduce the number of colors captured to 256.</p> <p>0 - Off 1 - On</p>	REG_DWORD	0
Compression Method	<p>Compression algorithm to use:</p> <p>1 - Enhanced 2 - Normal</p> <p>Note: For compatibility with HTML5 replay, additional compression methods supported by previous releases are no longer available.</p>	REG_DWORD	1
Compression Quality	<p>Compression Quality in the range 1 to 10</p> <p>10 - Best compression (Low Performance) 1 - Less Compression (Best Performance)</p> <p>Note: This setting is only applicable when 'CompressionMethod' is 1.</p>	REG_DWORD	5

Registry Entry	Description	Type	Default Value
Data Encryption	<p>If this entry is set to "1", Capture encrypts the screen data before sending it to the recorder server.</p> <p>0 - Not Encrypted 1 - Encrypted</p>	REG_DWORD	0
DualMonitor	<p>Add this setting if it is missing in the registry. Values include:</p> <p>0 - Dual monitor recording disabled 1 - Dual monitor recording enabled</p> <p>See Enable multi-monitor Screen Capture support (page 174) for specific details on the dual monitoring recording support.</p>	REG_DWORD	1
Enhanced Resolution	<p>Causes Capture to continuously fake a constant monitor to artificially use CPU and memory resources even when a monitor is not in progress:</p> <p>0 - Off 1 - On</p>	REG_DWORD	0

Registry Entry	Description	Type	Default Value
Integration Services ServerList	<p>Comma-delimited or semicolon-delimited list of Integration Services server names and ports the Capture Service uses. The Capture Service only connects to the first eight (8) hosts within the list.</p> <p>This registry entry maintains the list of Recorder Integration Service servers used to connect with the Verint proprietary protocol. This connection protocol is replaced with a new interface in 15.2 HFR3. If the connecting Recorder Integration Service in this list supports the new interface, the client automatically attempts to upgrade the connection to the newer interface. In order to maintain backwards compatibility and fallback connectivity, the entries are not removed from this registry. Even though entries are not removed from this registry key, the client only maintains one (1) connection to the Recorder Integration Service server.</p> <p>Example: hostname1:port1,hostname2:port2,hostname3:port3</p>	REG_SZ	""
MaxAvgCPU	The setting limits the amount of CPU (in percents) the capture can use.	REG_DWORD	60
Screen Change Detection Interval	<p>This setting defines how often (in msec) the capture checks for screen changes. The setting range is 25–500.</p> <p>Lowering the value increases the capture quality and the amount of CPU used by capture.</p> <p>Capture can automatically adjust the setting if the CPU utilization exceeds the value set by the MaxAvgCPU.</p>	REG_DWORD	150

Registry Entry	Description	Type	Default Value
Secure Cloud Integration Services Server List	<p>Comma-delimited or semicolon-delimited list of Integration Services server names and ports that the Capture Service uses to connect using a <i>secure</i> protocol. The Capture Service only connects to the first eight (8) hosts within the list.</p> <p>This registry entry controls how Screen Capture connects to the Recorder Integration Service and is applicable to both on-premises and cloud environments. Screen Capture supports automatic migration to this connection protocol and populates this setting with servers from the "Integration Services Server List" registry that supports the new interface.</p> <p>A given server should exist in either the "Cloud Integration Services Server List" or the "Secure Cloud Integration Services Server List", but not both. A server may continue to have an entry in the "Integration Services Server List" for fallback connectivity.</p> <p>Example: hostname1:port1,hostname2:port2</p>	REG_SZ	""
SSAR_BlockUnknownProcesses	<p>Used for Selective Screen Application Recording to block a process that cannot be identified (such as when run as administrator).</p> <p>0 - Do not block unknown processes 1 - Block unknown processes</p>	REG_DWORD	1
SSAR_ExcludeWholeScreenApps	<p>Excludes the specified application window from selective screen processing.</p> <p>Example: A customer is using an transparent overlay application that covers the whole window, including blacklisted applications. The name of the transparent overlay application can be added to this setting to prevent it from revealing any blacklisted application.</p> <p>Value is regular expression of application name, such as '<i>OverlayApp.exe</i>'.</p>	REG_SZ	—

Registry Entry	Description	Type	Default Value
SSAR_ListType	<p>Used for Selective Screen Application Recording to identify the applications on the agent screen that will or will not be recorded. Applications on the screen that are not recorded display in gray.</p> <ul style="list-style-type: none"> 0 - Do not record list All applications are recorded <i>except</i> for those identified in SSAR_Processes, SSAR_URLs, and SSAR_WindowsCaptions. The desktop is recorded. 1 - Record list All applications in SSAR_Processes, SSAR_URLs, and SSAR_WindowsCaptions are recorded. The desktop is not recorded. <p>Note: If a value other than 0 or 1 is used, or the SSAR_ListType registry entry is not found, the Selective Screen Application Recording feature is disabled.</p>	REG_DWORD	—
SSAR_Processes	<p>Based on SSAR_ListType setting, list of processes that will or will not be recorded. Examples: The first example prevents the entry from being ignored since regex is case-sensitive.</p> <pre>[oO][uU][tT][lL][oO][oO][kK]\\.[eE][xX][eE]</pre> <pre>outlook\exe</pre> <p>Note: The SSAR_Processes registry configuration does <i>not</i> support Universal Windows Platform (UWP) applications.</p>	REG_SZ	—

Registry Entry	Description	Type	Default Value
SSAR_SupportedBrowsers	<p>Optional. Limits the browsers supported by Selective Screen Application Recording to reduce the time spent querying all windows on the desktop from the root level node.</p> <p>Requires a comma-separated list of one or more of the following supported browsers:</p> <ul style="list-style-type: none"> • microsoftedge (Edge HTML) • msedge (Edge Chromium) • chrome • firefox <p>From the names listed in SSAR_SupportedBrowsers, the specific browser expression implementation is added to the ProcessMonitor for processing.</p> <p>If SSAR_SupportedBrowsers is blank or missing, all supported browsers are processed.</p>	REG_SZ	—
SSAR_TaskViewName	<p>Used with Windows 10 to prevent the Task View preview (Windows Key+Tab) from being recorded when Selective Screen Application Recording is enabled.</p> <p>For the language in use by the Windows operating system, enter the Windows title for Task View. For example, English is "Task View".</p>	REG_SZ	—
SSAR_URLs	<p>Based on SSAR_ListType setting, list of URLs that are or are not recorded.</p> <p>Example: www\company\com</p>	REG_SZ	—

Registry Entry	Description	Type	Default Value
SSAR_WindowsCaptions	<p>Based on SSAR_ListType setting, list of Windows captions (title for a dialog box) that are or are not recorded.</p> <p>The filter for Windows captions can include a bounding box description. The bounding box description is the amount of pixels it crops by. The bounding box, which includes (left right top bottom), specifies how the Windows bounds are cropped.</p> <p>Example: Registry Value Types</p>	REG_SZ	—
WebServerEnable	<p>When enabled, recording site updates are sent from the Recorder Integration Service (RIS) to the desktop. The configuration is used by the Capture Service and other applications that are running on the same desktop to receive notification messages from the RIS.</p> <p>Enable or disable the local web server.</p> <ul style="list-style-type: none"> • 1 - Enabled Capture service attempts to open the web server defined in the registry. • 0 - Disabled Capture service does not open the web server. <div> <p>i This setting must be added manually with WebserverMaxClients, WebServerPort, and WebServerRequireAuthentication.</p> </div>	REG_DWORD	1

Registry Entry	Description	Type	Default Value
WebServerMaxClients	<p>Maximum number of clients allowed to connect to the localhost web server. Once the maximum is reached, other clients that attempt to connect are rejected with a 503 error code.</p> <div> This setting must be added manually with WebServerEnable, WebServerPort, and WebServerRequireAuthentication.</div>	REG_DWORD	
WebServerPort	<p>Listen port for the localhost web server. Valid port range: 1-65535</p> <ul style="list-style-type: none">• If the web server is enabled and the port is within the valid range, the Capture Service attempts to open the web server on the localhost.• If the web server is disabled or the port is outside the valid range, the Capture Service does not attempt to open the web server. <div> This setting must be added manually with WebServerEnable, WebServerMaxClients, and WebServerRequireAuthentication.</div>	REG_DWORD	29479

Registry Entry	Description	Type	Default Value
WebServerRequireAuthentication	<p>Used to enable or disable enforcement of the authorization header on connecting clients.</p> <ul style="list-style-type: none"> 1 - Enabled All incoming client connections are required to have a valid authorization header. Any clients that attempt to connect without a header are rejected with a 401 error code. 0 - Disabled Incoming client connections without an authorization header are accepted. <p>Note: Whether enabled or disabled, a client with an authorization header is validated. If enforcement is disabled, but the authorization header cannot be validated, the connection is rejected.</p> <div>  This setting must be added manually with WebServerEnable, WebServerMaxClients, and WebServerPort. </div>	REG_DWORD	1
WSSPath	Directory path to the "agent.wss" file used by WCapW32.exe during server authentication and data encryption.	REG_SZ	""

Related topics

[Filter rules for Selective Screen Application Recording \(page 152\)](#)

[Selective Screen Application Recording registry example \(page 155\)](#)

Screen Capture specific entries

Changing the values of certain registry entries affects Screen Capture performance, recording quality, and network bandwidth usage.

Setting the appropriate registry values based on the Agent workstation configuration makes the Screen Capture Module operate most efficiently.



If you need to improve the screen recording image quality, contact your service representative.

Compression Method

The following table lists the supported compression methods and their metrics.

Compression Method	Avg. Compression Ratio
Normal Compression	8:1
Enhanced Compression	40:1

For compatibility with HTML5 replay, additional compression methods supported by previous releases are no longer available.



Note the following regarding compression:

- The compression ratio varies, depending on the screen bitmaps being compressed.
- Compression methods providing better compression ratio usually use more CPU.

CompressionQuality

The CompressionQuality entry is applicable only when 'Enhanced Compression' is used.

A setting of "10" produces the best compression quality and the smallest packets. It uses slightly more CPU. This setting conserves the most bandwidth but reduces the quality of the screen images when they are played back.

A setting of "1" results in lower quality compression. This setting uses the most network bandwidth and produces the best image quality when the recorded screen images are played back.

ColorReduction

New installations of the Screen Capture Module have the ColorReduction value set to "1" (on). However, upgrade installations of the Screen Capture Module keep the existing ColorReduction value.

When color reduction is enabled, the captured desktop bitmap data is converted to 8-bit color pixel data. Color reduction usually causes loss of data quality as fewer colors are displayed on playback.

The advantage of color reduction is that it results in smaller packets. Smaller packets result in less network bandwidth and disk space for screen capture files.

Color reduction is more suitable when the agents are using Notepad, Word, and Outlook (including other applications of this type). Such applications produce less color data.

ScreenChangeDetectionInterval

The ScreenChangeDetectionInterval defines how often (in msec) the capture checks for screen changes. The setting range is 25–500.

The default value is 150; the suggested value is 50.

Lowering the value increases the capture quality, but also increases the amount of CPU used by capture.

Filter logon types for Screen Capture Agent

Windows server generates logon events each time an agent logs on. The Screen Capture Agent uses these logon events to determine when to start recording. Unrelated processes running on the same workstation triggers extra user logon events. Extra logon events cause the Screen Capture Agent to start recording unnecessarily, possibly even dropping an agent currently being recorded.

Identify extra logon events

- integrationservice.log - You can identify the events causing the false triggering of Screen Capture by examining the integrationservice.log file on the server. See "Log Manager Utility" in the *Recorder Configuration and Administration Guide*.
- integrationservice.log - Alternatively, if nothing is found in integrationservice.log, check the CaptureService.log file on the agent side.

After identifying extra logon events

Using the provided procedure, create a filter that tells Screen Capture to ignore those events by adding a registry key.

Windows Logon Events

The complete list of Windows Logon Events is as follows (refer to Microsoft's documentation for more information):

- 2 Interactive
- 3 Network
- 4 Batch
- 5 Service
- 7 Unlock
- 8 NetworkCleartext
- 9 NewCredentials
- 10 RemoteInteractive
- 11 CachedInteractive

Logon/logoff messages are only sent to the Recorder server for users not blocked by the filter created in the registry. If you do not enter any data for this registry setting, logon/logoff messages are sent for all users.

Procedure

1. On the workstation where the capture Service is installed, run **regedit**.
 - For 32-bit operating system, navigate to:
`[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion]`
 - For 64-bit operating system, navigate to:
`[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\eQuality Agent\Capture\CurrentVersion]`
2. Add a registry key named **FilterLogonTypes**.

3. As the Data for this key, enter the numeric representation of the Logon Event(s) you want to exclude from messages sent to the Recorder server, separated by commas.

Example: FilterLogonTypes 4,5,7

Filter rules for Selective Screen Application Recording

Selective Screen Application Recording is configured to record all applications listed (Record List) or to record all applications except for those applications listed (Do not record list). To configure Selective Screen Application Recording, you must add several registry entries, including regular expressions to filter the applications being recorded.

Windows 11 installations

If Selective Screen Application Recording is being used, make sure that the SSAR Process, Caption, and URL registry entry configurations are correct. Some operating system files are named different from previous operating system versions.

Supported browsers

Edge HTML

Edge Chromium

Google Chrome

Firefox

Things you need to know about the “Do not record list”

If the SSAR_ListType=0,

- While the SSAR_URLs, SSAR_WindowsCaptions, and SSAR_Processes filters are independent, the SSAR_Processes filters take precedence over the other two.
Example: If chrome.exe is in the “Do not record” SSAR_Processes list, all instances of Chrome are grayed out, regardless of SSAR_URLs or SSAR_WindowsCaptions entries.
- If SSAR_WindowsCaptions values include a bounding box, the filtered window is cropped based on the parameters provided.

Things you need to know about the “Record list”

If the SSAR_ListType=1,

- If SSAR_URLs and SSAR_WindowsCaptions filtering are being used, there is a dependency on the SSAR_Processes filter. In addition to the SSAR_URLs or SSAR_WindowsCaptions filters, define the applicable process in SSAR_Processes.
Example: If a URL should be recorded, then the browser (such as iexplorer.exe) must be included in the SSAR_Processes list.
- If SSAR_WindowsCaptions filter is being used, the software tries to match the listed captions for all listed process filters. In this case, captions you do not want to exclude might be excluded.

Examples:

If "Registry editor" should be included, add "Registry editor" to the SSAR_WindowsCaptions list. In addition, add regedit.exe to the SSAR_Processes list since this is the process that displays the Registry editor window.

If the caption is not static, for example a text editor that displays the file name and path, you must include each possible caption in the list.

If one or more captions are defined in SSAR_WindowsCaptions, you must include every caption you want to record in SSAR_WindowsCaptions.

For example, in Microsoft Edge, if the only entry in SSAR_WindowsCaptions is "weather", all tabs in Microsoft Edge that include the word "weather" are recorded. All other tabs are not recorded.

- If a bounding box is attached to the end of the SSAR_WindowsCaptions regular expression, the selected Window is cropped based on the parameters provided. The cropping parameters are associated with the bounding box as (left right top bottom). The bounding box parameters are separated by a blank space.
- If SSAR_Processes includes "chrome" and SSAR_URLs does *not* include any URLs, then the entire Chrome browser process is white listed.
- If SSAR_Processes includes "chrome" and SSAR_URLs includes URLs, then the Chrome browser is white listed for the URLs included in SSAR_URLs.
- If SSAR_Processes does *not* include "chrome" and SSAR_URLs includes URLs, then Chrome and Edge browsers are white listed for the URLs included in SSAR_URLs.



For Windows 8, Windows 10, Windows 2016 and above, for Selective Screen, the Start menu is not detectable. If using the "Do not record list", the Start menu is always blocked. If using the "Record list," the Start menu cannot be filtered out.

Procedure

1. Before you add the registry entries and their regular expressions, it is recommended that you test the regular expressions. The following URLs can be used to test the regex strings.

<https://regex101.com/>

<http://www.rubular.com/>

Examples:

Expression	Result
<code>^.*company\.com</code>	All addresses in the <i>company.com</i> domain are allowed.
<code>^(?!privat.)*\.*company\.com</code>	All addresses in the <i>company.com</i> domain are allowed, except for <i>privat.company.com</i> . The address <i>privat.company.com</i> is not included because of the exclamation point in the <i>(?!privat)</i> condition.

Expression	Result
<code>^shop.*\company\.com</code>	<p>All addresses in the domain <i>company.com</i> that meet the following criteria are allowed:</p> <ul style="list-style-type: none"> • start with <i>shop</i> • end with <i>.company.com</i> <p>Also includes <i>shop.company.com</i>, where <i>*</i> is a wildcard, including empty entries.</p>
<code>^www[1-3]\company\.com</code>	<p>All addresses in the following domains are allowed:</p> <ul style="list-style-type: none"> • <i>www1.company.com</i> • <i>www2.company.com</i> • <i>www3.company.com</i>
<code>^www[a-z]\company\.com</code>	<p>Similar to the above, with letters instead of numbers. Examples:</p> <ul style="list-style-type: none"> • <i>wwwa.company.com</i> • <i>wwwb.company.com</i> • <i>wwwc.company.com</i>

Regular expression characters used in the examples:

- ^ Start of new line
- . Any single character
- * Zero or more characters
- \. Dot character

Where: \ is an escape character in regular expressions.

- On the workstation where the capture Service is installed, run regedit.
- For a 32-bit system, navigate to:
[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion]
 For a 64-bit system, navigate to:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\eQuality Agent\Capture\CurrentVersion]
- To turn Selective Screen Application Recording on, add the following registry key:
[SSAR_ListType \(page 145\)](#)
- Based on the SSAR_ListType setting, add the following registry keys, including the regular expressions used to specify the filtering rules:
[SSAR_Processes \(page 145\)](#)
[SSAR_URLs \(page 146\)](#)

[SSAR_SupportedBrowsers \(page 146\)](#)

[SSAR_WindowsCaptions \(page 147\)](#)



To add multiple values to a regular expression filtering rule, separate the values with a , (comma). The key is valid when any of the comma-separated values are valid.

Example: To specify multiple values (Microsoft Outlook and Notepad) for SSAR_Processes, the regular expression is:

outlook\.exe, notepad\.exe

6. After installing and configuring the Selective Screen Application Recording registry entries, the desktop must be restarted for the feature to work.
7. You can test the entries are correct by stopping monitoring, modifying the registry setting, and then monitoring a session with CapTest. The registry entries are "read" when a screen capture session is started.

Related topics

[Screen Capture registry values \(page 139\)](#)

[Selective Screen Application Recording registry example \(page 155\)](#)

Related information

Regular-Expressions.info (<http://www.regular-expressions.info>)

Selective Screen Application Recording registry example

The Windows Registry example shows several *Do not record list* entries. The SSAR_Processes entry excludes Outlook.exe, no matter whether entries are or are not capitalized on each workstation. The SSAR_WindowsCaptions entry excludes all windows whose dialog box title is Calculator.

Why does the example show two backslashes?

Note in the example below, that the registry adds a second backslash (\) when a backslash is used. That is why the export example below contains two backslashes (\\).

Example

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality
Agent\Capture\CurrentVersion]
```

```
"SSAR_URLs"="^.*shop\\.company\\.com"
```

```
"SSAR_Processes"="[wW][iI][nN][wW][oO][rR][dD]\\.[eE][xX][eE]"
```

```
"SSAR_WindowsCaptions"="Calculator (10 10 10 10)"
```

```
"SSAR_ListType"=dword:00000000
```

Related topics[Screen Capture registry values \(page 139\)](#)[Filter rules for Selective Screen Application Recording \(page 152\)](#)

Registry values for Terminal Services support

The registry values for Terminal Services Screen Capture support for 32-bit and 64-bit systems are provided.

32-bit system

[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion]

64-bit system

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\eQuality Agent\Capture\CurrentVersion]

Additional registry keys

The following additional registry values are applicable only when Screen Capture Module Service is running on Terminal Services Server.

Registry Entry	Description	Type	Default Value
TermSvr	Used to indicate thin-client server: 0 - Not Terminal Server 1 - Terminal Server	REG_DWORD	1
ServiceSocketListenPort	Capture service socket port for listening for recorder server connections in Terminal Services environments. Typically 4002.	REG_DWORD	4002

AIM registry values

The location of the AIM registry keys for a 32-bit system and a 64-bit system are provided.

32-bit system

[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\AIM]

64-bit

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\AIM]

Registry values

Agent Initiated Monitoring uses the following registry values.

Registry Entry	Description	Type	Default Value
Enable Annotation	Enables the Annotate option in the AIMTray menu.	REG_DWORD	1
Automated LogonLogoff	Used to enable or disable Automatic Logon/Logoff of the user. 1 - Enable 0 - Disable	REG_DWORD	1
StartStop Behavior	Specifies events that are sent for Start Monitoring and Stop Monitoring commands: Start monitoring events 0 - StartRecord 1 - Connected 2 - Connected, StartRecord Stop monitoring events 0 - StopRecord 1 - Disconnected 2 - StopRecord, Disconnected	REG_DWORD	0
StartStop ContentType	Specifies media type for Start and Stop Monitoring commands: AudioVideo - audio and screens Audio - audio only Video - screens only	REG_SZ	Audio Video
Start Monitoring	Used to display or hide the "Start Monitoring" option in the AIM menu tray. 1 - Display 0 - Hide	REG_DWORD	1
Stop Monitoring	Set this value to 1 to display the Stop Monitoring option in AIMTray menu. 1 - Display 0 - Hide	REG_DWORD	1

Registry Entry	Description	Type	Default Value
Block Monitoring	Set this value to 1 to display the Block Monitoring option in the AIMTray menu. 1 - Display 0 - Hide	REG_DWORD	1
UserField Name1	Specifies the User Field 1 custom attribute name.	REG_SZ	Contact .AIM. User1
UserField Name2	Specifies the User Field 2 custom attribute name.	REG_SZ	Contact .AIM. User2
UserField Name3	Specifies the User Field 3 custom attribute name.	REG_SZ	Contact .AIM. User3
UserField Name4	Specifies the User Field 4 custom attribute name.	REG_SZ	Contact .AIM. User4
UserField Name5	Specifies the User Field 5 custom attribute name.	REG_SZ	Contact .AIM. User5
UserField1	Specifies the User Field 1 label name in the Annotation dialog box.	REG_SZ	""
UserField2	Specifies the User Field 2 label name in the Annotation dialog box.	REG_SZ	""
UserField3	Specifies the User Field 3 label name in the Annotation dialog box.	REG_SZ	""
UserField4	Specifies the User Field 4 label name in the Annotation dialog box.	REG_SZ	""
UserField5	Specifies the User Field 5 label name in the Annotation dialog box.	REG_SZ	""
UserTip1	Specifies the text that appears for the User Field 1 tooltip in the Annotation dialog box.	REG_SZ	This is user field 1

Registry Entry	Description	Type	Default Value
UserTip2	Specifies the text that appears for the User Field 2 tooltip in the Annotation dialog box.	REG_SZ	This is user field 2
UserTip3	Specifies the text that appears for the User Field 3 tooltip in the Annotation dialog box.	REG_SZ	This is user field 3
UserTip4	Specifies the text that appears for the User Field 4 tooltip in the Annotation dialog box.	REG_SZ	This is user field 4
UserTip5	Specifies the text that appears for the User Field 5 tooltip in the Annotation dialog box.	REG_SZ	This is user field 5
Start Monitoring Annotation FieldName1	Specifies the field name that is tagged in Start Monitoring command. Note: Manually add these settings if they are missing from the Registry.	REG_SZ	""
Start Monitoring Annotation FieldName2		REG_SZ	""
Start Monitoring Annotation FieldName3		REG_SZ	""
Start Monitoring Annotation FieldName4		REG_SZ	""
Start Monitoring Annotation FieldName5		REG_SZ	""

Registry Entry	Description	Type	Default Value
Stop Monitoring Annotation FieldName1	Specifies the field name that is tagged in Stop Monitoring command. Note: Manually add these settings if they are missing from the Registry.	REG_SZ	
Stop Monitoring Annotation FieldName2		REG_SZ	
Stop Monitoring Annotation FieldName3		REG_SZ	
Stop Monitoring Annotation FieldName4		REG_SZ	
Stop Monitoring Annotation FieldName5		REG_SZ	

Registry Entry	Description	Type	Default Value
Block Recording Annotation FieldName1	Specifies the field name that is tagged in Block Recording command. Note: Manually add these settings if they are missing from the Registry.	REG_SZ	
Block Recording Annotation FieldName2		REG_SZ	
Block Recording Annotation FieldName3		REG_SZ	
Block Recording Annotation FieldName4		REG_SZ	
Block Recording Annotation FieldName5		REG_SZ	

Registry Entry	Description	Type	Default Value
Pause Recording Annotation FieldName1	Specifies the field name that is tagged in Pause Recording command. Note: Manually add these settings if they are missing from the Registry.	REG_SZ	
Pause Recording Annotation FieldName2		REG_SZ	
Pause Recording Annotation FieldName3		REG_SZ	
Pause Recording Annotation FieldName4		REG_SZ	
Pause Recording Annotation FieldName5		REG_SZ	
ResumeRecording Annotation FieldName1	Specifies the field name that is tagged in Resume Recording command. Note: Manually add these settings if they are missing from the Registry.	REG_SZ	
ResumeRecording Annotation FieldName2		REG_SZ	
ResumeRecording Annotation FieldName3		REG_SZ	
ResumeRecording Annotation FieldName4		REG_SZ	
ResumeRecording Annotation FieldName5		REG_SZ	

Registry Entry	Description	Type	Default Value
StartMonitoring Annotation FieldValue1	Specifies the field value that is tagged in Start Monitoring command. Note: Manually add these settings if they are missing from the Registry.	REG_SZ	""
StartMonitoring Annotation FieldValue2		REG_SZ	""
StartMonitoring Annotation FieldValue3		REG_SZ	""
StartMonitoring Annotation FieldValue4		REG_SZ	""
StartMonitoring Annotation FieldValue5		REG_SZ	""
StopMonitoring Annotation FieldValue1	Specifies the field value that is tagged in Stop Monitoring command. Note: Manually add these settings if they are missing from the Registry.	REG_SZ	
StopMonitoring Annotation FieldValue2		REG_SZ	
StopMonitoring Annotation FieldValue3		REG_SZ	
StopMonitoring Annotation FieldValue4		REG_SZ	
StopMonitoring Annotation FieldValue5		REG_SZ	

Registry Entry	Description	Type	Default Value
BlockRecording Annotation FieldValue1	Specifies the field value that is tagged in Block Recording command. Note: Manually add these settings if they are missing from the Registry.	REG_SZ	
BlockRecording Annotation FieldValue2		REG_SZ	
BlockRecording Annotation FieldValue3		REG_SZ	
BlockRecording Annotation FieldValue4		REG_SZ	
BlockRecording Annotation FieldValue5		REG_SZ	
PauseRecording Annotation FieldValue1	Specifies the field value that is tagged in Pause Recording command. Note: Manually add these settings if they are missing from the Registry.	REG_SZ	
PauseRecording Annotation FieldValue2		REG_SZ	
PauseRecording Annotation FieldValue3		REG_SZ	
PauseRecording Annotation FieldValue4		REG_SZ	
PauseRecording Annotation FieldValue5		REG_SZ	

Registry Entry	Description	Type	Default Value
ResumeRecordingAnnotationFieldValue1	Specifies the field value that is tagged in Resume Recording command.	REG_SZ	""
ResumeRecordingAnnotationFieldValue2	Note: Manually add these settings if they are missing from the Registry.	REG_SZ	""
ResumeRecordingAnnotationFieldValue3		REG_SZ	""
ResumeRecordingAnnotationFieldValue4		REG_SZ	""
ResumeRecordingAnnotationFieldValue5		REG_SZ	""
EnableAnnotationCleaning	Set to 1 to clear the Annotation field values every time the annotation dialog is opened. If it is set to 0, then AIM preserves the Annotation field values from the last time they were specified.	REG_DWORD	1
ShowIcon	Set this value to 1 to display the AIMTray icon on the task bar. Set this value to 0 if needed only in QM environments where AIM can be configured to send automated login/logoff messages to BDR Server. For Recorder server environments, always set to 1.	REG_DWORD	1
HideExitMenuItem	Set this value to 1 to hide the Exit option in the AIMTray menu. 1 - Hide 0 - Display	REG_DWORD	0

Registry Entry	Description	Type	Default Value
PauseMonitoring	Set this value to 1 to enable the Pause and Resume Monitoring options in the AIMTray Menu. 1 - Enable 0 - Hide	REG_DWORD	1
PauseResume ContentType	Specifies media type for Pause and Resume Recording commands: AudioVideo - audio and screens Audio - audio only Video - screens only	REG_SZ	Audio Video

Configuration required to support AIM call annotation

You can enable Agent Initiated Monitoring (AIM) during the Screen Capture Module installation. If you enable AIM, you must also perform additional configurations to ensure that agents can annotate calls from AIM.

Workflow

1. [Configure AIM to support annotations \(page 168\)](#)
Configuring AIM to support annotations should be performed during the Screen Capture Module installation. If it is not performed during the Screen Capture Module installation, it can also be accomplished by altering the Screen Capture Module registry settings after the product is installed.
2. [Configure custom attributes in Enterprise Manager \(page 169\)](#)
After you have provided values for the User Field X settings, as described in [Configure AIM to support annotations](#), you must create custom attributes for each of the user fields.
3. [Enable custom data fields and mapping attributes \(page 171\)](#)
After you have configured attributes in the Enterprise Manager, you must enable five Custom Data fields and then map the attributes to those Data Fields.
4. [Configure custom data in the adapter \(page 172\)](#)
Configuring custom data fields in the adapter is the fourth of five procedures associated with ensuring that agents can annotate calls with AIM.
5. [Verify the configuration is working \(page 172\)](#)
Verifying that the configuration is working is the last procedure associated with ensuring that agents can annotate calls with AIM. After performing the previous procedures, annotate a call to verify that the configuration is working.

Configure AIM to support annotations

Configuring AIM to support annotations should be performed during the Screen Capture Module installation. If it is not performed during the Screen Capture Module installation, it can also be accomplished by altering the Screen Capture Module registry settings after the product is installed.

Procedure to configure annotation during product installation

1. Complete the following settings on the **Integration Services Options** installation screen:
 - a. Select the **Connect to Integration Services** option.
 - b. In the **Connect Adapter URL <hostname:port>** field, you must specify the hostname and port of the server that hosts the Integration Service server role.

This configuration is required to connect to the Integration Service to send logon/logoff and other AIM messages to the Integration Service.

2. On the **AIM Annotation Setup** installation screen, complete the **User Field X** settings (**User Field 1**, **User Field 2**, **User Field 3**, **User Field 4**, and **User Field 5**).

The values you enter in these fields will appear to the agent in the user interface when the agent annotates the call. In this example, assume that you make these entries in the five User Field settings:

- Customer Name
- Address
- Phone
- Issue
- Notes



For complete installation instructions, see [Screen Capture and AIM \(page 99\)](#).

Procedure to configure annotation after product installation

Alternately, if you did not configure the User Field X settings during the Screen Capture Module installation, or if you configured them incorrectly, you can configure them from the registry editor after the Screen Capture Module is installed.

1. Start the registry editor on the computer on which the Screen Capture Module is installed (**Start > Run** and type **regedit**).
2. Depending on the operating system, open
 - For 32-bit operating system:
`[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\AIM]`
 - For 64-bit operating system:
`[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\AIM]`

3. Enter values for the following registry keys. The values you enter for each of these registry keys will appear to the agent in the user interface when the agent uses AIM to annotate the call:
 - UserField1
 - UserField2
 - UserField3
 - UserField4
 - UserField5
4. Restart the AIM application.
 - a. Right click the AIM icon in the system tray and click **Exit**.
 - b. Run the AimTray.exe file (located in the directory in which the Screen Capture Module is installed).

Related topics

[Configuration required to support AIM call annotation \(page 167\)](#)

Configure custom attributes in Enterprise Manager

After you have provided values for the User Field X settings, as described in [Configure AIM to support annotations](#), you must create custom attributes for each of the user fields.

Naming custom attributes

The names of these custom attributes must *exactly* match the names that are specified for the UserFieldNameX registry keys on the computer that hosts the Screen Capture Module application.

It is recommended that you create custom attribute names that match the default names provided for the UserFieldNameX registry keys, as discussed in the procedure below.

Before you begin

[Configure AIM to support annotations \(page 168\)](#)

Procedure

1. The default values for each of the five **UserFieldNameX** registry keys are shown below:

Registry Key	Default Value
UserFieldName1	Contact.AIM.User1
UserFieldName2	Contact.AIM.User2
UserFieldName3	Contact.AIM.User3
UserFieldName4	Contact.AIM.User4
UserFieldName5	Contact.AIM.User5



To view these registry keys and their current settings, run the registry editor on the computer on which the Screen Capture/AIM application is installed.

For 32-bit system, open: [HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\AIM].

For 64-bit system, open: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\AIM]

2. Create custom attributes with names that exactly match the values associated with the **UserFieldNameX** registry entries.
 - a. In the Enterprise Portal application, select **Recording Management**. Under **Custom Data**, select **Attributes**.
 - b. Select the **Create** button (in the bottom right corner).
 - c. In the **Name** field, type the name that matches the value associated with registry key **UserFieldName1** (in this example, type **Contact.AIM.User1**). You can accept the remaining default entries on the **New Attribute** screen, or alter them as needed.
 - d. Select the **Save** button.
 - e. Repeat steps b. through d., to create four more default custom attributes with names that match the values of the **UserFieldName2** through **UserFieldName5** registry keys.

When you are finished, the following five attributes should display under the **Custom** heading at the bottom of the **Attributes** screen.

 - Contact.AIM.User1
 - Contact.AIM.User2
 - Contact.AIM.User3
 - Contact.AIM.User4
 - Contact.AIM.User5

Related topics

[Configuration required to support AIM call annotation \(page 167\)](#)

Enable custom data fields and mapping attributes

After you have configured attributes in the Enterprise Manager, you must enable five Custom Data fields and then map the attributes to those Data Fields.

Before you begin

[Configure custom attributes in Enterprise Manager \(page 169\)](#)

Procedure

1. In the Enterprise Portal application, select **Interaction**. Under **Administration**, select **Custom Data**.
2. Enable five Custom Data fields, one for each custom attribute that you configured in [Configure custom attributes in Enterprise Manager \(page 169\)](#). You can enable any five Custom Data fields that are not currently enabled. In this example, we will enable Custom Data fields 1 through 5.
 - a. Select the icon in the **Edit** column for Custom Data 1, and then select the **Enabled** option to enable the Custom Data 1 field.
 - b. From the **Data Source** list, select the data source from which the data was received:
 - For a CTI integration, select **CTI**.
 - For an API integration, select **API**.
 - For DPA event triggers, select **Screen Analysis**.
 - c. Repeat step a. and step b. to enable the fields Custom Data 2 through Custom Data 5.



You can enable any five of the 300 available Custom Data fields. It is not mandatory to enable the Custom Data 1 through 5 fields.

At this point, you have enabled the Custom Data fields. Next, you must map attributes to the Custom Data fields you have just enabled.

3. In the Enterprise Portal application, select **Recording Management**. Under **Custom Data**, select **Custom Data Mapping**.

Each Custom Data field that you enabled displays in the Custom Data screen. For example, if you enabled Custom Data fields 1 through 5, you will see CDF1, CDF2, CDF3, CDF4, and CDF5 displayed.

4. In the **Attribute Mapping** column, map each of the 5 CDFs to one of the Custom Attributes that you created in [Configure custom attributes in Enterprise Manager \(page 169\)](#).

Example:

- For CDF1, in the Attribute Mapping column select Contact.AIM.User1.
- For CDF2, in the Attribute Mapping column select Contact.AIM.User2.
- For CDF3, in the Attribute Mapping column select Contact.AIM.User3.
- For CDF4, in the Attribute Mapping column select Contact.AIM.User4.
- For CDF5, in the Attribute Mapping column select Contact.AIM.User5.

Related topics[Configuration required to support AIM call annotation \(page 167\)](#)

Configure custom data in the adapter

Configuring custom data fields in the adapter is the fourth of five procedures associated with ensuring that agents can annotate calls with AIM.

Before you begin[Enable custom data fields and mapping attributes \(page 171\)](#)**Procedure**

1. In Recorder Manager, select **General Setup**. Under **Integration Adapters**, select **Attributes**.
2. Select the adapter from the left pane.
3. Find the custom data field and set its value. For example:
 - For custom data field Contact.AIM.User1, set it to Attributes.Contact.AIM.User1.
 - For custom data field Contact.AIM.User2, set it to Attributes.Contact.AIM.User2.
 - For custom data field Contact.AIM.User3, set it to Attributes.Contact.AIM.User3.
 - For custom data field Contact.AIM.User4, set it to Attributes.Contact.AIM.User4.
 - For custom data field Contact.AIM.User5, set it to Attributes.Contact.AIM.User5.

Related topics[Configuration required to support AIM call annotation \(page 167\)](#)

Verify the configuration is working

Verifying that the configuration is working is the last procedure associated with ensuring that agents can annotate calls with AIM. After performing the previous procedures, annotate a call to verify that the configuration is working.

Before you begin[Configure custom data in the adapter \(page 172\)](#)**Procedure**

1. On the computer where the Screen Capture Module is installed, use the AIM feature to start the audio or the audio and screen recording. (Make sure the computer where AIM is running is part of the workspace.)

2. When annotating a call from AIM, verify that the **Annotate Call** dialog displays the values that you specified for User Fields 1 through 5 in the procedure [Configure AIM to support annotations \(page 168\)](#). In this example, those values included:
 - Customer Name
 - Address
 - Phone
 - Issue
 - Notes
3. In the **Annotate Call** dialog, enter an annotation for each of the five fields listed in the previous step and then click the **OK** button to send the annotation tagging.
4. Stop the call.
5. In the Portal, open the contact and verify that the Custom Data fields display the same values that you entered for each of the five fields in step 3.

If the Custom Data fields display the same values you entered in the five fields in step 3, the AIM call annotation feature is working correctly.

Related topics

[Configuration required to support AIM call annotation \(page 167\)](#)

Troubleshoot the configuration

You can use the Integration Service log and the audio call XML file as troubleshooting tools if the AIM annotation feature is not working correctly.

Locate errors

- Integration Service log - locate the IEMessage that contains the attributes of the AIM annotation message, and examine the attributes for errors.
- Audio call XML file - examine the <tag> attribute associated with the call annotation for possible errors.

Enable multi-monitor Screen Capture support

Screen Capture Module can record screens from multiple monitors attached to a workstation. Recording multiple monitors is controlled by the DWORD registry setting **DualMonitor**.

32-bit system

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality  
Agent\Capture\CurrentVersion]
```

64-bit system

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\eQuality  
Agent\Capture\CurrentVersion]
```

DualMonitor registry setting

- If **DualMonitor** is set to **1**, Screen Capture Module records video from all attached monitors. There can be more than two monitors attached to a workstation. By default, **DualMonitor** is set to **1**.
- If **DualMonitor** is set to **0**, Screen Capture Module only records video from the designated primary monitor screen.

Set the appropriate value for **DualMonitor** as needed.

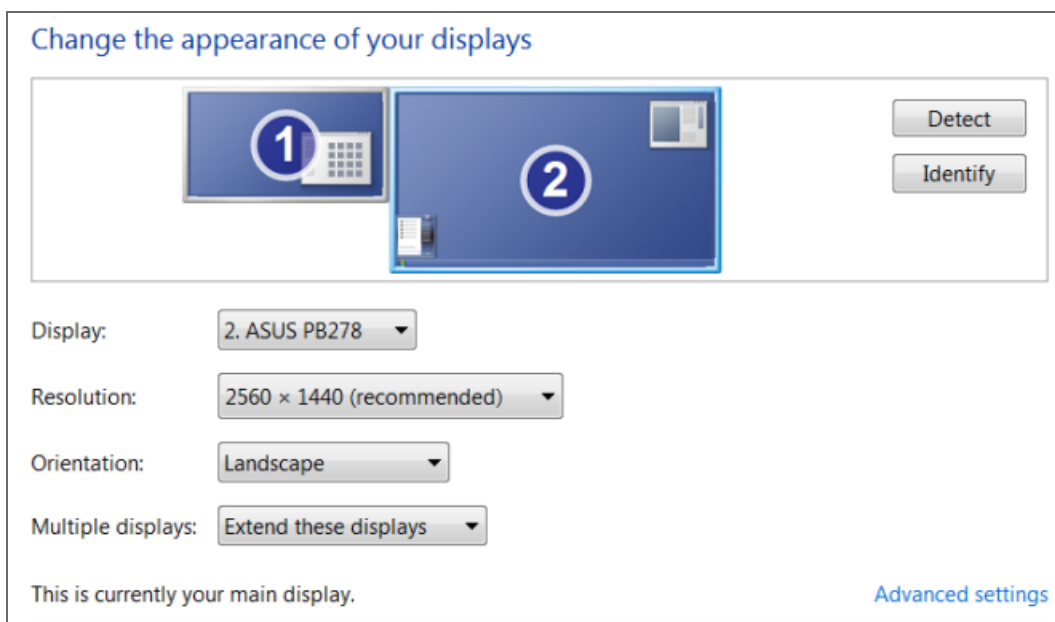
- Capturing video from multiple monitors increases the network bandwidth utilization.
- Monitors can have different resolutions. Recorded screen width will equal the sum of all monitor widths. Recorded screen height will equal the maximum height from all monitor heights.

Configuration tested

Screen capture of multiple monitors is tested in the following configuration:

- Multiple monitors are attached to a single display adapter.
- Multiple monitors are configured by selecting the **Multiple displays > Extend these displays** option in the Change the appearance of your display dialog box.

If the monitors are attached to more than one display adapter, then the behavior is unknown. In general, the Screen Capture Module captures all the monitors in the sequence displayed in the Change the appearance of your displays dialog.



Encrypt screen recordings in-transit

For V15.2 systems, encryption of captured screen data is managed through HTTPS communications with server and CA certificates and NOT through the "Encryption screen recordings in-transit" setting in Enterprise Manager.

The "Encryption screen recordings in-transit" setting in Enterprise Manager is only used when the screen recorder OR screen capture module is on V15.1. In this case, encryption is managed through .wss files.

Related information

For V15.2: Data In-Transit Encryption (*Security Configuration Guide*)

For V15.1: Encrypt Screen Recordings In-Transit (V15.1 only) (*Security Configuration Guide*)

Use a proxy server for screen capture

You can configure the screen capture module to use a proxy server to access the recorders and Recorder Integration Service. Accessing recorders through a proxy server secures the recorders from random access in cloud environment.

Before you begin

The proxy server must be configured and running.

Procedure

1. Following the standard installation procedure, install the Screen Capture Module.
2. To the Screen Capture Module registry, under **[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Witness Systems\eQuality Agent\Capture\CurrentVersion]**, add a value for the key, **ProxyServer**.
Example: **ProxyServer=10.156.2.149:3128**



The presence of the **ProxyServer** key in the registry indicates that the installed version of the Screen Capture Module supports the use of a proxy server. If the key is not present, the installed Screen Capture Module version does not support a proxy server.
If the **ProxyServer** key value is blank, the Screen Capture Module runs without a proxy server.

3. Restart the machine.

Related topics

[Install Screen Capture and AIM manually \(page 99\)](#)

Screen capture proxy for live monitoring on Chrome configuration

Desktop live monitoring on Chrome in a secured environment requires a certificate that is trusted by the clients with screen live monitoring and configured on the desktops that run the screen capture module.

For a description of how the target desktop is proxied through a screen recorder server for Real-time Monitoring, see the Technical Overview.



To establish connection to the Secure Web Socket, verify the following:

If the root CA certificate **sslsocket.verint.com** does not exist, contact Service to generate the root CA certificate for the first start. Then, add this root CA certificate to all client workstations to the **Trusted Certificate Authorities** folder.

Related information

Real-Time Monitoring Data Flow (*Technical Overview*)

Known issues for the Screen Capture module

This section discusses Screen Capture Module configuration notes and known issues.

Known issues

- [Windows 7 Terminal Server issue \(page 179\)](#)
- [Windows 7 and Windows 2008 R2 issues \(page 180\)](#)
- [Remote Desktop connection issue \(page 180\)](#)
- [Windows Media Player capture issue \(page 180\)](#)
- [Bandwidth usage and disk storage space conservation with Screen Capture \(page 181\)](#)
- [Upgrades do not change the ColorReduction registry setting \(page 181\)](#)
- [Screen stitching within segment not supported \(page 182\)](#)
- [Screen Capture module failed to capture screens \(page 182\)](#)
- [Screen Capture module failed to capture screen and application data \(page 183\)](#)
- [Black screen when playing a large screen file on a dual monitor \(page 183\)](#)
- [Black screen in SCN file after disabling monitor \(page 183\)](#)
- [Color palette change in Aero mode on Windows 7 \(page 183\)](#)
- [Agent screen resolution modification during recording is not supported \(page 183\)](#)
- [Selective Screen Application Recording: Aero Peek, Alt+Tab, and Win Key+Tab not supported \(page 184\)](#)
- [Agent screen display settings change requires system restart \(page 184\)](#)

Windows 7 Terminal Server issue

The following issue occurs when the Screen Capture Module is installed on the Windows 7 Terminal Server Operating Systems.

The LogManager.exe file must run as an administrator or it will display an empty list of components. This problem occurs even when the LogManager.exe runs under an Administrator account.

To fix this problem, do either of the following:

- Run the Logger as Administrator:
 1. In Windows Explorer, go to **\Program Files\Witness Systems\Screen Capture Module** directory.
 2. Hover over the **LogManager.exe** file and select **Run as Administrator** from the right-click menu.
- Using **regedit32**, give the user account that runs **LogManager.exe** full access to the **[HKEY_LOCAL_MACHINE\SOFTWARE\Witness\Tracing]** registry key.

Windows 7 and Windows 2008 R2 issues

Issues might occur when the Screen Capture Module is installed on Windows 7 or Windows 2008 R2, and the Windows User Account Control (UAC) settings are enabled.

Issues

- The LogManager.exe file must run as Administrator if you want to change the log settings. See [Windows 7 Terminal Server issue \(page 179\)](#) for instructions on running LogManager.exe as Administrator.
- If programs (such as captureService.exe or wcapw32.exe) have problems generating log files, you must provide the logged in user with the permissions needed to create files in the folder where the log files are stored (this folder is specified during the Screen Capture Module installation).

Resolution

If the UAC settings are disabled in the operating system, neither of the issues above will occur. One way to disable the UAC settings is described.

Procedure

1. Go to Windows **Control Panel**.
2. In the **Search** box, type **UAC**.
3. Select **Change User Account Control settings**.
4. On the **User Account Control Settings** dialog, move the slider down to the lowest value so that it is positioned at the **Never notify** setting.
5. Select **OK**.
6. Restart the computer to disable the User Access Control settings.

Remote Desktop connection issue

If a Remote Desktop session is being recorded, and the user minimizes the Remote Desktop window to the taskbar, a black screen is recorded.

Example: Black screen is recorded in this scenario

1. The user accesses an application over a Remote Desktop Connection.
2. The Screen Capture Module begins recording the session.
3. The user minimizes the Remote Desktop Connection window to the taskbar.

Windows Media Player capture issue

The Screen Capture Module cannot capture movie files (such as .mpeg or .avi files) played in Windows Media Player when the **Use overlays** option is selected in the Video Acceleration settings of Media Player.

If the **Use overlays** option is selected, a black screen appears inside the Windows Media Player when the screen is captured (and the screen recording is played back). To prevent this problem, disable the Use overlays option in Windows Media Player.

Procedure

1. Open Windows Media Player.
2. Select **Tools**, and then select **Options**.
3. Select the **Performance** tab.
4. Select the **Advanced...** button.
5. In the Video Acceleration section, clear the check mark from the **Use overlays** setting.
6. In the Video Acceleration Settings window, select **OK**.
7. In the Options window, select **Apply**, and then select **OK**.
8. In the Video Acceleration Settings window, select **OK**.
9. In the Options window, select **Apply**, and then select **OK**.

The Use overlays option is disabled.

Bandwidth usage and disk storage space conservation with Screen Capture

When the Screen Capture application captures screen data, the captured screen data is both transmitted on the network to the screen recorder and then archived in files on a storage server.

Reduce bandwidth and disk space

You can reduce the network bandwidth consumed by the transmission of screen image data on the network, and also reduce the disk space required to store the screen recordings. To accomplish this, adjust the Display settings of the computer on which the screen capture is performed, as noted below:

- Use lower Display resolution settings
- Use simple Background images on the desktops

High resolution settings and complex background images cause more data to be created during the capture process, and result in more data being transmitted on the network and saved to disk.

Upgrades do not change the ColorReduction registry setting

New installations of the Screen Capture Module set the ColorReduction value to 1. However, upgrade installations of the Screen Capture Module will keep the existing ColorReduction value.

ColorReduction registry setting

System Administrators can change the ColorReduction setting in the registry by opening the registry editor and navigating to the parameter.

32-bit system

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality  
Agent\Capture\CurrentVersion]:ColorReduction
```

64-bit system

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Witness Systems\eQuality  
Agent\Capture\CurrentVersion]:ColorReduction
```

Screen stitching within segment not supported

Stitching of multiple screen recordings within a segment is not supported. During playback of the recorded segment, only the first screen recording is played back.

Example: Using START/STOP commands to control recording

When a customer uses the START/STOP commands to control recording for PCI compliance, audio and screen recordings are segmented. If the agent presses START, STOP, START during a call, the result is two (2) audio and two (2) screen recording segments. In this case the system stitches the audio and concatenates them into one audio segment, however the two screen recordings are not stitched. During playback this results in the audio playing back seamlessly, while only the first screen recording is played back.

Workaround

In this scenario, the customer should be advised to use PAUSE/RESUME commands. This prevents the screen segmentation and during playback the full screen recording is displayed.

Screen Capture module failed to capture screens

While screen recording using Remote Display Protocol (RDP), the Screen Capture module failed to capture screens, resulting in a black screen displaying during playback.

Issue

Some graphic cards do *not* support the WDDM video driver. For these video cards, the WDDM video driver must be disabled by changing a registry setting. Disabling the setting, causes the Remote Desktop Connection to use the XDDM video driver.

Workaround

1. On the workstation where the capture service is installed, run **regedit**.
2. Go to:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services
```
3. For the **fEnableWddmDriver** policy setting, disable the driver by changing the value from 1 to **0**.
4. Restart the computer.

Screen Capture module failed to capture screen and application data

The Screen Capture module implements various low level Windows operating system hooks and API calls to capture screen and application data.

Issue

One such API that Screen Capture uses is Microsoft's Desktop Duplication API (MS DDAPI). At 'some' customer sites the type of remote desktop client used to access a remote desktop can interfere with the MS DDAPI and therefore Screen Capture functionality.

Workaround

Contact Customer Support. Screen Capture can be configured to use a different Windows API 'BitBlit' in combination with a custom dirty rectangle code to work around this MS DDAPI limitation.

Black screen when playing a large screen file on a dual monitor

When playing a large screen file on a dual monitor (where both the Supervisor and the Agent have a dual screen), and extracting the screen window to be shown on the supervisor's secondary monitor, the agent's primary monitor is shown correctly, but when scrolling to the agent's secondary monitor, the playback displays a black screen.

Workaround

Use the Fit to Screen option to fit the image size to the monitor size. This enables the image to display properly (although it may appear a little smaller).

Black screen in SCN file after disabling monitor

If using multiple monitors and one monitor is disabled, the screen capture agent restarts internally. The restart occurs in order to acquire the screen frames. While the restart occurs, the SCN file includes approximately 15 seconds of blank recording.

Color palette change in Aero mode on Windows 7

When Aero mode is enabled on Windows 7 the colors of recorded screens are distorted.

Workaround

Disable Aero mode on Windows 7 for better screen recording.

Agent screen resolution modification during recording is not supported

Agent screen resolution modification during recording is not supported in all operating systems.

Agent screen size modification is not supported

Capture does not support the agent resizing, maximizing, or restoring a terminal session window. Agents should always have the session window maximized. If the window dimensions change, Capture might miss some of the screen activity.

Selective Screen Application Recording: Aero Peek, Alt+Tab, and Win Key+Tab not supported

Aero Peek, Alt+Tab, and the Windows Key+Tab are blacklisted when Selective Screen Application Recording is enabled.

Agent screen display settings change requires system restart

When Selective Screen Application Recording is used on an agent desktop, you must restart the agent desktop after the screen display settings (such as changing from landscape to portrait) are changed.

CapTestB utility

The CapTestB Utility is typically installed on an IT Administrator workstation for testing the performance of the screen capture application installed on the Agent Workstation for Recording.

Related topics

[Introducing the CapTestB utility \(page 185\)](#)

[Run the CapTestB utility \(page 186\)](#)

[Performance analysis \(page 190\)](#)

Introducing the CapTestB utility

CapTestB is a test utility used with the Screen Capture Module. CapTestB allows you to view screen activity from a remote agent session and gather valuable performance measurements.

You can use this utility to test connectivity, gauge network performance, and to test image quality provided by the agent capture software. You can then further analyze the information gathered to determine the best possible configuration settings for agent capture in your particular environment.

Test configuration settings

The “Agent Override” option allows you to upload test configuration settings to the agent capture software and view performance differences without ever having to alter the agent's workstation. These overrides take effect for the duration of the test monitor and then revert to the local settings.

Measurements are recorded to file every minute, and the file can be saved at the end of the test session to retain for further analysis.

CapTestB security

CapTestB has a built-in security feature to prevent unauthorized usage. Whenever a test monitor is attempted, a pop-up dialog appears on the agent's workstation alerting the agent that a test monitor is about to take place. The message text displayed indicates the workstation that is attempting to perform the test. This feature is provided to eliminate privacy concerns within your organization.

To suppress the pop-up, security dialog box

If enterprise policy does not require an Agent response when running CapTestB, you can suppress the pop-up dialog box when running a test monitor.

1. On the workstation where the screen capture application is installed, go to the following key in the Windows registry:

HEY_LOCAL_MACHINE/Software/Wow6432Node/Witness Systems/eQuality Agent/Capture/CurrentVersion

2. Add the following entry to the registry at the key location from the previous step:

Type: **DWORD**

Name: **TestMonitorAuthorization**

Value: **0**



To reinstate the default behavior of providing a security notification on the desktop, remove the DWORD entry above from the registry.

CapTestB system requirements

For operating system requirements for CapTestB, refer to [Supported operating systems \(page 20\)](#).

Run the CapTestB utility

The CapTestB main window contains a control bar (left frame), statistics grid (lower frame) and playback window for viewing screen captures.

Before you begin

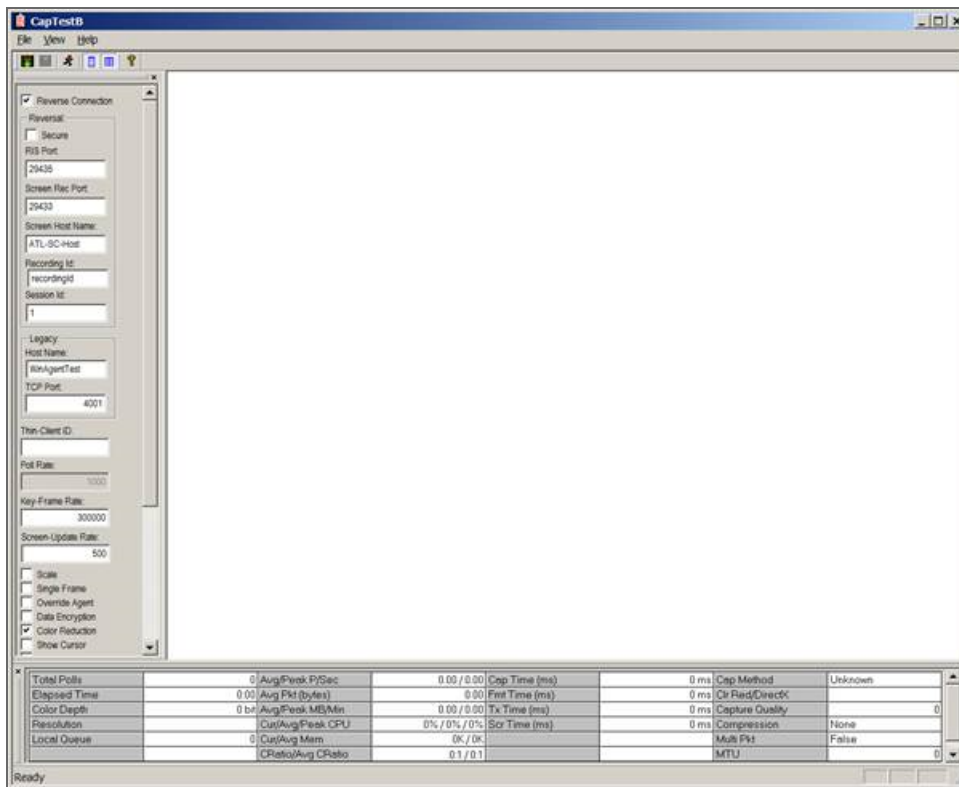
Copy the .wss file created by the client to the CapTestB tool folder. If the system is using Data-in-transit encryption for screen recordings, the file must be named server.wss.

Procedure

1. Copy the **Captest.zip** file to a workstation that is not an Agent Desktop installed with the Screen Capture module.
2. Extract the files to a local folder.
3. Run the utility by double-clicking **captest.exe**.

If the utility fails to run, install the Microsoft Visual C++ 2015 Redistributable or Microsoft Visual C++ 2015 application file (available from <http://www.microsoft.com>), and then run **captest.exe** again.

The CapTestB Utility opens to the main window.



4. Configure the control bar with test parameters and agent workstation parameters.
See [Control bar \(page 187\)](#)
5. From the **File** menu, select **Start Monitor**. Or, on the toolbar, select **Start**.
In most configurations, an alert appears on the workstation informing the user that the utility is attempting to monitor the workstation. Select **OK**.
Screen Capture performance statistics appear in the Statistics Grid. See [Statistics grid \(page 189\)](#) for a description of each statistic.
6. Analyze screen capture performance. The performance statistics are color coded to reflect threshold and danger levels.
See [Performance analysis \(page 190\)](#)
7. Delete the **Captest.zip** and the extracted files after use.

Control bar

The Control Bar is used to input CaptestB configuration parameters and Agent Workstation Screen Capture configuration parameters. In addition, CapTestB supports both legacy connections and the Selective Screen Application Recording connection mechanism.

When using CapTestB with Selective Screen Application Recording, you must:

- Configure your Agent Capture registry for Selective Screen Application Recording (see *Cloud Integration Services Server List* and *Secure Cloud Integration Services Server List* in [Screen Capture registry values \(page 139\)](#)).
- Select the **Reverse Connection** check box in CapTestB.

Reverse Connection (Selective Screen Application Recording) configuration parameters

- **Reverse Connection:** Select to place CapTestB in connection reversal mode for Selective Screen Application Recording.
- **Secure:** Select to make CapTestB use TLS certificates for communication. If using this option, you must place your server.pem and serverKey.pem certificate files in your CapTestB directory.
- **RIS Port:** The RIS port number which CapTestB opens for incoming Agent Capture Connections.
- **Screen Rec Port:** The Screen Recorder port number CapTestB receives captured screen data on.
- **Screen Host Name:** The host name CapTestB is running on. The Screen Host Name is used by Agent Capture to connect back to CapTestB as if it were a screen recorder.
- **Recording ID:** Unique recording ID to identify this CapTestB session in the logs (for example, TestId1).
- **Session Id:** The Agent Capture session to capture. Defaults to first agent logon session of 1.

Legacy configuration parameters

- **Host Name:** Host name of the agent's workstation or the host name of a thin-client server.
- **TCP Port:** TCP connection port number. 4001 for workstations and 4002 for thin-client servers.

Common configuration parameters

- **Thin-Client ID:** Host name of a thin-client device if using host ID mode, or the Agent's Windows NT logon ID if using agent ID mode. Leave empty for workstation monitoring.
- **Poll Rate:** Rate (in milliseconds) to poll for changes.
- **Key-Frame Rate:** Rate (in milliseconds) to poll for key-frames.
- **Scale:** Select to scale image display to fit within the playback window.
- **Single Frame:** Select to display each delta frame individually.
- **Override Agent:** Select to use agent overrides for the next test session.
- **Data Encryption:** Select to encrypt captured screen files while in transit.
- **Color Reduction:** Select to reduce captured color to 8-bit (256 colors).

Agent workstation Screen Capture parameters

- **Agent Capture Version:**
- **Capture Quality:** Desired capture quality setting from 1 to 10.
- **Compression:** Desired compression method: 1=Witness Enhanced, 2=Witness Standard
- **Compression Quality:** Desired compression quality setting from 1 to 10.
- **Recording ID:** Unique recording ID to identify this CapTest session in the logs (for example, TestId1).
- **Session Id:** Agent Capture session to capture. Defaults to first agent logon session of 1.

Related topics

[Screen Capture registry values \(page 139\)](#)

Statistics grid

The performance statistics are reported in the statistics grid.

Performance statistics

- **Total Polls:** the total number of polls sent by CapTestB to the agent.
- **Elapsed Time:** the total amount of time since the beginning of this monitor session.
- **Color Depth:** the color depth of the agent's session.
- **Resolution:** the screen resolution of the agent's session.
- **Local Queue:** the size of the receive queue on the local workstation.
- **Avg/Peak Pkts/Sec:** the average and the peak number of packets received from agent capture per second.
- **Avg/Peak MB/Min:** the average and the peak mega-bytes received from agent capture per minute. By creating a sample agent recording and then examining this data, you can determine the bandwidth usage of Screen Recording. See the Performance and Sizing Guidelines for bandwidth requirements.
- **Curr/Avg/Peak Rem CPU:** the current, average, and peak CPU usage by WCapW32.exe on the agent's workstation.
- **Curr/Avg Rem Mem:** the current and the average memory usage by WCapW32.exe on the agent's workstation.
- **CRatio/Avg CRatio:** the compression ratio and the average compression ratio of the compressed image size to the uncompressed image size.
- **Capture Time (ms):** the amount of time in milliseconds required to capture sample image data from the agent's screen.
- **Format Time (ms):** the amount of time in milliseconds required to format the captured data for transmission.
- **Transmit Time (ms):** the amount of time in milliseconds required to transmit a packet from the agent's workstation to CapTestB.
- **Screen Time (ms):** the amount of time in milliseconds required to capture the entire screen.
- **Cap Method:** the Detection Method currently in-use on the agent's workstation.
- **Clr Red/DirectX:** indicates whether color reduction or DirectX capture is enabled on the remote workstation.
- **Capture Quality:** indicates the capture quality setting on the remote workstation.
- **Compression:** the compression method currently in-use on the agent's workstation.
- **Multi-Pkt:** indicates whether multi-packet is enabled on the remote workstation.
- **MTU:** the setting for maximum transmission unit currently in-use on the agent's workstation.

Performance analysis

Performance analysis involves gathering statistics for different configuration sets and selecting the optimal settings for the given environment. There are typically three objectives to choose from.

Objectives

- Agent impact
- Recording quality
- Journal-file size

The choices you make will favor one of these objectives. For this reason, it is important for you to have a clear understanding of your objectives and trade-offs in order to make an informed choice.

Statistic threshold values

Several of the statistics are assigned warning and danger threshold values. If measurements exceed these thresholds, the background color of the grid cell changes to yellow or red. The statistics and their threshold values are listed in the table.

Statistic	Warning	Danger
Local Queue Size	10	15
Average Packets Per Sec.	6	9
Average Packet Size	20,000 bytes	30,000 bytes
Average MB Per Min.	10 MB	15 MB
Remote CPU	20%	30%
Remote Memory	10,000 KB	15,000 KB
Capture Time	20 ms	30 ms
Format Time	20 ms	30 ms
Transmit Time	200 ms	300 ms
Screen Time	1000 ms	1500 ms

No matter what your objective, strive to stay below warning thresholds. In extreme cases, staying below thresholds is not possible and you will have to sacrifice performance. In any case, a careful analysis of statistics gathered helps you determine the most optimal settings and problem areas within the recording environment.

Media Encoder

If the Plugin Player is not installed or access is not available to the Portal, use Media Encoder to convert audio files to a PCM-encoded .wav format. Installing and enabling the conversion option is described.

Topics

Media Encoder overview	192
Convert audio files	193

Media Encoder overview

Using the Media Encoder, it is possible to convert audio files to a PCM-encoded .wav format for workstations inside or outside the organization that are not installed with the Plugin Player or cannot access the Portal.

Installation prerequisites

Microsoft .NET Framework 4.6.1 or higher is required.

Installing the Media Encoder

The Media Encoder is part of the playback application installation package. To install the playback application, see [Player \(page 86\)](#).

Media Encoder installation location

C:\Program Files\<Company Name>\Playback\CommandLineConvertor

Convert audio files

You can convert audio files to the PCM-encoded .wav format either from the command line or by adding a right-click menu convert option. This allows the user to download audio files recorded by the system locally, right-click the file to convert it to a media file, and send it to a workstation that does not have Plugin Player or the proprietary compressed codec installed.

 The Media Encoder does not support the conversion of encrypted files.

Related topics

[Enable the convert option \(page 193\)](#)

[Disable the convert option \(page 194\)](#)

[Convert from the command line \(page 194\)](#)

Enable the convert option

This is relevant for workstations running Windows Operating Systems only.

Procedure

1. Open a text editor (such as Notepad) and create a new text file.
2. Copy the following text into the text file:
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\SoundRec\shell\&Avaya_convert]
@="&Avaya_convert"
[HKEY_CLASSES_ROOT\SoundRec\shell\&Avaya_convert\command]
@="\"C:\\Program Files\\Avaya\\Playback\\CommandLineConvertor.exe\" \"%L\""
3. If the Plug Player is installed at a different location on your computer, change the path to the CommandLineConvertor.exe file.
4. Save the text file with a .reg extension and close the file.
5. Open the file and click **Yes** to add the information to the registry shell.
6. Verify that the **Avaya convert** option appears when you right-click an audio file.

 Avaya Media Encoder does not support the conversion of encrypted files.

7. Delete the file that you created at step 4.
8. You can now download system audio files locally, right-click the file to convert it to a media file and send it to workstation that does not have the Plugin Player or Avaya Codec installed.

Disable the convert option

You can disable the convert-click open in the Windows menu.

Procedure

1. From the workstation that includes the Convert option, run the following command:
`CommandLineConvertor -UnRegShell`
2. Verify that the **Avaya convert** option does not appear in the menu when you right-click an audio file.

Convert from the command line

You can run the convert option from the command line. You can then send the converted output file to a workstation that does not have the Plugin Player or Avaya Codec installed.

Procedure

1. Run the following command:
`cd [Path to the Media Encoder application file] CommandLineConvertor [inputFileName] [outputFileName]`

The parameters are described in the following table:

Parameter	Description
Path to the Media Encoder application file	Default location is: C:\Program Files\<company name>\Playback
CommandLineConvertor	Media Encoder application file name.
inputFileName	Full path and name of the audio file you want to convert.
outputFileName	Full path and name of the converted file. If you do not supply an output, Media Encoder creates one by adding Conv to the source file name. For example, input_Conv.wav
/? or no parameter	For help. Displays the Media Encoder application name.

Example:

```
cd C:\Program Files\<company name>\Playback CommandLineConvertor
C:\My Media Files\originals\input.wav C:\My Media
Files\converted\output.wav
```