IMPACT360®

Desktop Applications

Deployment Reference and Installation Guide

Version 11.1
Document Revision 1.10

VERINT®

All materials (regardless of form and including, without limitation, software applications, documentation, and any other information relating to Verint Systems, its products or services) are the exclusive property of Verint Systems Inc. Only expressly authorized individuals under obligations of confidentiality are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by Verint Systems, and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

The Verint Systems Inc. products are protected by one or more of the following U.S., European or International Patents: USPN 5,659,768; USPN 5,790,798; USPN 6,278,978; USPN 6,370,574; USPN 6,404,857; USPN 6,510,220; USPN 6,724,887; USPN 6,751,297; USPN 6,757,361; USPN 6,782,093; USPN 6,952,732; USPN 6,959,078; USPN 6,959,405; USPN 7,047,296; USPN 7,149,788; USPN 7,155,399; USPN 7,203,285; USPN 7,216,162; USPN 7,219,138; USPN 7,254,546; USPN 7,281,173; USPN 7,284,049; USPN 7,325,190; USPN 7,376,735; USPN 7,424,715; USPN 7,424,718; USPN 7,466,816; USPN 7,478,051; USPN 7,558,322; USPN 7,570,755; USPN 7,574,000; USPN 7,587,041; USPN 7,613,290; USPN 7,633,930; USPN 7,634,422; USPN 7,650,293; USPN 7,660,307; USPN 7,660,406; USPN 7,660,407; USPN 7,672,746; USPN 7,680,264; USPN 7,701,972; USPN 7,734,783; USPN 7,752,043; USPN 7,752,508; USPN 7,769,176; USPN 7,774,854; USPN 7,787,974; USPN 7,788,286; USPN 7,792,278; USPN 7,792,671; USPN 7,801,055; USPN 7,817,795; USPN 7,822,018; USPN 7,826,608; USPN 7,836,171; USPN 7,848,524; USPN 7,853,006; USPN 7,852,994; USPN 7,853,800; USPN 7,853,753; USPN 7,864,946; USPN 7,873,156; USPN 7,881,216; USPN 7,881,471; USPN 7,882,212; USPN 7,882,217; USPN 7,885,813; USPN 7,899,178; USPN 7,899,180; USPN 7,899,176; USPN 7,904,481; USPN 7,903,568; USPN 7,904,325; USPN 7,907,142; USPN 7,913,063; USPN 7,920,482; USPN 7,925,889; USPN 7,930,314; USPN 7,949,552; USPN 7,953,621; USPN 7,953,719; USPN 7,953,750; USPN 7,965,828; USPN 7,966,397; USPN 7,991,613; USPN 7,995,612; USPN 8,000,465; USPN 8,005,676; USPN 8,015,042; USPN D606,983; USPN RE40,634; USPN RE41,534; USPN RE41,608; AU 2003214926; CA 2,474,735; CA 2,563,960; CA 2,564,127; CA 2,564,760; CA 2,567,232; CA 2,623,178; CA 2,627,060; CA 2,627,064; CA 2,628,553; EP 1096382; EP 1248449; EP 1284077; DE 1284077; FR 1284077; DE 833489; FR 833489; GB 833,489; GB 2374249; IE 84821; IE 85519; IL 13532400; NZ 534642; ZL 200520118289.3; ZL 200520118288.9; ZL 200520118287.4; USPN D606,983; USPN RE40,634; USPN RE41,534; USPN RE41,608; AU 2003214926; CA 2,474,735; CA 2,563,960; CA 2,564,127; CA 2,564,760; CA 2,567,232; CA 2,623,178; CA 2,627,060; CA 2,627,064; CA 2,628,553; EP 1096382; EP 1248449; EP 1284077; DE 1284077; FR 1284077; DE 833489; FR 833489; GB 833,489; GB 2374249; IE 84821; IE85519; IL 13532400; NZ 534642; ZL 200520118289.3; ZL 200520118288.9; ZL 200520118287.4; and other provisional rights from one or more of the following Published U.S. Patent Applications: US 10/061,491; US 10/467,899; US 10/633,357; US 11/166,630; US 11/345,587; US 11/359,195; US 11/359,319; US 11/359,356; US 11/359,357; US 11/359,358; US 11/359,532; US 11/361,208; US 11/388,944; US 11/394,408; US 11/394,410; US 11/394,794; US 11/395,759; US 11/475,683; US 11/477,124; US 11/478,714; US 11/479,056; US 11/479,267; US 11/479,506; US 11/479,899; US 11/509,549; US 11/509,550; US 11/540,107; US 11/540,185; US 11/540,320; US 11/540,900; US 11/540,902; US 11/567,808; US 11/567,852; US 11/583,381; US 11/608,340; US 11/608,350; US 11/608,358; US 11/616,490; US 11/621,134; US 11/691,530; US 11/692,983; US 11/693,828; US 11/693,923; US 11/693,933; US 11/712,933; US 11/723,010; US 11/742,733; US 11/752,458; US 11/776,659; US 11/824,980; US 11/831,250; US 11/831,257; US 11/831,260; US 11/831,634; US 11/844,759; US 11/872,575; US 11/924,201; US 11/937,553; US 11/959,650; US 11/968,428; US 12/015,375; US 12/015,621; US 12/053,788; US 12/055,102; US 12/057,442; US 12/057,476; US 12/107,976; US 12/118,789; US 12/118,792; US 12/164,480; US 12/245,781; US 12/326,205; US 12/351,370; US 12/416,906; US 12/464,694; US 12/466,673; US 12/483,075; US 12/497,793; US 12/497,799; US 12/504,492; US 12/539,640; US 12/608,474; US 12/628,089; US 12/630,030; US 12/684,027; US 12/686,213; US 12/708,558; US 12/725,127; US 12/753,137; US 12/762,402; US 12/768,194; US 12/792,796; US 12/840,227; US 12/840,233; US 12/852,144; US 12/879,868; US 12/887,059; US 12/887,089; US 12/888,445; US 12/891,620; US 12/915,868; US 12/915,941; US 12/916,006; US 12/940,508; US 12/942,111; US 12/964,891; US 13/005,996; US 13/008,283; US 13/011,870; US 13/011,871; US 13/016,998; US 13/036,923; US 13/096,145; US 13/096,148; US 13/096,153; US 13/114,620; US 13/149,655; US 13/155,343; US 13/182,672; US 13/187,438; US 13/189,514; and other U.S. and International Patents and Patents Pending.

Certain components of this Software or software contained in this Product (collectively, "Software") may be covered by so-called "free or open source" software licenses ("Open Source Components"), which includes any software licenses approved as open source licenses by the Open Source Initiative or any similar licenses, including without limitation any license that, as a condition of distribution of the Open Source Components licensed, requires that the distributor make the Open Source Components available in source code format. A license in each Open Source Component is provided to you in accordance with the specific license terms specified in their respective license terms. EXCEPT WITH REGARD TO ANY WARRANTIES OR OTHER RIGHTS AND OBLIGATIONS EXPRESSLY PROVIDED DIRECTLY TO YOU FROM VERINT, ALL OPEN SOURCE COMPONENTS ARE PROVIDED "AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

Any third party technology that may be appropriate or necessary for use with the Verint Product is licensed to you only for use with the Verint Product under the terms of the third party license agreement specified in the Documentation, the Software or as provided online at to://verint.com/thirdpartylicense. You may not take any action that would separate the third party technology from the Verint Product. Unless otherwise permitted under the terms of the third party license agreement, you agree to only use the third party technology in conjunction with the Verint Product.

Visit our website at www.verint.com/intellectualpropertynotice for updated information on Verint Intellectual Property.

Document Revision 1.10
Published January 28, 2013

Contents

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.

Using Desktop Applications:

- Agent screens are captured and saved together with recordings
- Agents can initiate recording
- Supervisors can playback recordings when browsing to the Portal
- Application Administrators can create forms that Supervisors and Managers use to evaluate and assess agents.
- Data is transferred between workstations and data center or site servers.
- Workstation logs are collected for use by technical support.

Intended Audience

This guide is designed to be used by:

- Verint Systems and Business Partner professional services staff responsible for planning and setting up systems.
- Customer System Administration and IT staff responsible for site preparation and installing workstations.
- Verint Systems Field Services and partners responsible for installing workstations as part of the installation and site acceptance testing.

Documentation Feedback

We strive to produce the highest quality documentation products and welcome your feedback. If you have comments or suggestions about our guides or online help, you can email us. Please include the following information with your feedback:

- Product name and version number
- Name of online help or guide
- Topic name and page number (if applicable)
- Brief description of content
- Your suggestion for correcting or improving the documentation

Please send your messages to userguides@verint.com.

The email address is only for documentation feedback. If you have a technical question, please contact Technical Support.

Technical Support

Our goal at Verint Systems is to provide you with the best products backed by a high-quality support network with a variety of resource options. Verint Systems Technical Support services include email and telephone support.

To learn more about the support options that best suit your needs, visit us at verint.com/EISsupport.

Verint University

In addition to documentation, online Help, and support services, Verint Systems also offers both classroom-based and online learning alternatives to suit your specific needs.

To learn more about available training options from Verint Systems, visit us at verint.com/training.

Chapter 1

Getting Started

Desktop Applications Installation Workflow

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

1 **Plan**: Which desktop applications require installing? See "Desktop Applications Matrix" on page 11.

2 **Prepare:** Ensure the desktops (end user machines) meet the minimum specifications. See Chapter 2 "Customer Requirements".

3 **Install:** Decide on the Installation Method. Desktop applications can be batch installed silently, or individual applications 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 Chapter 3 "Installation by Role: Silent Distribution".

- **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 Chapter 4 "Installation by Application"

4 **Administer:** System administration of the desktop application is required at times, when configuring site dependent playback or when server name changes need to be reflected in the desktop application configuration registry. See Chapter 6 "System Administration for Desktop Applications"

5 **Upgrade:** If upgrading to desktop applications compatible with systems from previous suite versions, follow the upgrade instructions. See Chapter 5 "Upgrading Desktop Applications". For upgrading Content Producer, see "Upgrading Content Producer" on page 46.

6 **Refer**: Refer the user to the relevant configuration, administration, or user guide. See Appendix D "Related Documentation".

Desktop Applications Matrix

The Desktop Applications Matrix provides a quick reference to the applications and their relevancy for the user. The applications required by each user are based on the default privileges of the predefined roles that are activated with all licensed systems.

Desktop Applications	**Function**	**Agents**	**Supervisors**	**Managers**	**Administrators and Analysts**
Desktop Resources	Desktop Resources is a prerequisite package that includes mandatory resources required by certain desktop applications. For a complete list of the desktop applications dependent on Desktop Resources, refer to "Software Dependencies between Desktop Applications" on page 25.	✓	✓	✓	✓
Playback	Required to playback audio and screen files from the Portal.		✓	✓	✓
Form Designer	Create and manage evaluation and assessment forms. *A Supervisor or Manager may require Form Designer if they have Administer privileges.		*	*	✓
Standalone Form Designer	Offline version of the Form Designer with modified functionality for customers that need to set up forms in advance of installing Interactions and Analytics.				
User Import Support Package	Imports individual users (not in bulk) from a Windows domain into the User Manager.				✓
Screen Recording (including AIM)	Trigger audio recording, screen capture and provides logging information.	✓			
Pop-up Notification System Client	Send notices to agents manually, or automatically based on performance parameters.				
Content Producer	Use to develop learning clips. Standalone product for developers of training content.				
Forecasting and Scheduling	Manage and plan contact center activities.		✓	✓	
Strategic Planner	Strategic resource planning.		✓	✓	
Phonetic Boosting	Enables you to add new terms/phrases to the Speech Recognition engine's pre-defined vocabulary and to boost the recognition of all terms/phrases that are part of your company's vocabulary.				✓
Real Time Speech Calibration Applications	Analyze and diagnose Real Time Speech Notification performance. Add pronunciations to terms and calibrate notification scoring methods.				✓
Desktop Gadgets	Displays Scorecard KPI information on the Desktop with near real time updates.	✓	✓	✓	✓

Desktop Applications	Function	Agents	Supervisors	Managers	Administrators and Analysts
Desktop and Process Analytics (DPA) Client	Captures desktop activity data according to defined rules and executes DPA triggers such as stop/start recording, message prompts, and guidance scripts.	✓			
DPA Process Discovery	Visio based reporting tool for DPA Analysts.				✓
Logger	View log information for troubleshooting purposes. *Agent Logging is also possible using the log component of the Screen Capture Module.	*	✓	✓	✓

Obtaining the Installation Packages

Following the release of the Desktop Installation DVD, up-to-date version of desktop application installation packages are downloaded from the **Verint Online for Customers** site, as follows**.**

1 Browse to **Impact 360 V11.1 > Support & Downloads > Latest Hotfixes and HFRs.**

2 Expand the Hotfixes Tree to **Impact 360 V11.1 > V11.1 > SPx** and filter by **Desktop.**

3 Select the relevant **Subsystem**, and then click the **Download Link** (format is KB1XXXXX).

4 In the Directory window, download the **KB11XXXX.zip**.

IMPORTANT For DPA clients, use the **DPA Installation DVD**. It contains both DPA server and DPA client installation packages.

Chapter 2

Customer Requirements

Operating Systems

- Windows Operating Systems, page 14
- Windows Security Settings, page 15
- Windows Firewalls, page 16
- Antivirus Settings, page 16

Windows Operating Systems

The following table lists the supported Operating Systems, for each Desktop Application installed on the end user machine.

	Windows 2008 64-bit, 32-bit, R2, R2 SP1	**Windows 7, 7 SP1 (64-bit/32-bit) (Ultimate, Enterprise, Business)**	**Windows Vista SP2 32-bit (Ultimate, Enterprise, Business)**	**Windows Vista SP1 32-bit (Ultimate, Enterprise, Business)**	**Windows 2003 SP1, SP2, R2 32-bit (Standard, Enterprise)**	**Windows XP SP3**	**Windows XP SP1, SP2**
Screen Capture Module (including AIM)	✓	✓	✓	✓	✓	✓	✓
Playback	✓	✓	✓	✓	✓	✓	✓
Form Designer	✓	✓	✓	✓	✓	✓	
Standalone Form Designer	✓	✓	✓	✓	✓	✓	
User Import Support Package	✓	✓	✓	✓	✓	✓	✓
Logger	✓	✓	✓	✓	✓	✓	✓
Pop-up Notification System Client		✓	✓	✓	✓		✓
Content Producer		✓	✓	✓	✓	✓	
Forecasting and Scheduling	✓	✓	✓	✓	✓	✓	✓
Strategic Planner		✓	✓		✓		✓
Phonetics Boosting		✓			✓	✓	✓
Real Time Speech Calibration Application	✓	✓	✓	✓	✓	✓	✓
Desktop Gadgets	✓	✓	✓	✓	✓	✓	✓
Desktop and Process Analytics (DPA) Client	✓	✓	✓	✓		✓	✓
DPA Process Discovery	✓	✓	✓	✓		✓	✓

Windows Security Settings

All Desktop Applications support SSL and non-SSL communication environments.

SEE ALSO Refer to the *Security Overview and SSL Configuration Guide* for Desktop Security Settings.

Elevating UAC Security

The Desktop Applications installation files must be run as a Windows Administrator. By default, the Windows Vista/7/2008 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.

To elevate UAC security in Windows Vista, Windows 7 and Windows 2008 Operating Systems:

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.

Prerequisites for Windows in a Domain Environment

- When installing the Desktop Applications on Windows Vista/7/2008 in a domain environment, the installation is required to be performed in the same domain or in a trusted domain.
- Since a Workgroup is not a trusted environment, install desktop applications in a Workgroup environment manually.
- In domain environments it is required to support the **Kerberos** authentication protocol. Refer to the Kerberos Authentication Protocol section in the *Technologies, Security, and Networking Deployment Reference Guide.*

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.

SEE ALSO

The firewall ports that require opening are listed in the *Firewall Ports Configuration* spreadsheet that is delivered together with the *Technologies, Security and Network Integration Deployment Reference Guide*. Ensure the Desktop platform is selected in order to view all Inbound and Outbound ports required.

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, the customer is required to set up the corresponding exclusions in the antivirus application being used.

SEE ALSO

Refer to the *Technologies, Security and Network Integration Deployment Reference Guide* for the list of antivirus settings required for Desktop Applications.

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.

The hardware specifications for terminal services are proportional to the number of simultaneous users accessing the terminal services. Take into consideration the user profile and the applications they use. See “Hardware Specifications” on page 18 for a list of hardware requirements per user role and per application where relevant.

The following table lists the supported thin client and VMware environments for each of the Desktop Applications:

	Windows 2008 R2/R2 SP1 64-bit Edition with Terminal Server enabled, and with 32-bit/64-bit Citrix XenApp 6.0	**Windows Server 2008 SP1/SP2 64-bit Edition with Terminal Server enabled, and with 32-bit/64-bit Citrix XenApp 5.0**	**Windows Server 2003 64-bit Edition with Terminal Server enabled, with 32-bit/64-bit Citrix XenApp 5.0/4.5 (formerly Presentation Server 4.5)**	**Windows Server 2008 R2 (Hyper-V)**	**Citrix XenApp 5.x/6.x XenDesktop 5.x/6.x**	**VMware View (VDI) 3.0, 3.1’ 4.x**	**Windows 2003 Terminal Services (any SP level)**	**Windows 2000 Terminal Services (any SP level)**	**Citrix MetaFrame XP Server (any feature release, any SP level, Win 2000 and Win 2003)**	**Citrix MetaFrame PS 3.0 and 4.0 Enterprise Edition (*), (Win 2000 and Win 2003)/Advanced Edition, (Win 2000 and Win 2003)**
Screen Capture Module (including AIM)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Playback	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Form Designer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Standalone Form Designer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
User Import Support Package	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Logger				✓	✓	✓	✓	✓	✓	✓
Pop-up Notification System Client	✓	✓	✓				✓			
Content Producer	✓	✓	✓							
Forecasting and Scheduling	✓	✓	✓				✓			
Strategic Planner	✓	✓	✓				✓			
Phonetics Boosting	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Real Time Speech Calibration Application	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Desktop Gadget	✓	✓	✓				✓			

	Windows 2008 R2/R2 SP1 64-bit Edition with Terminal Server enabled, and with 32-bit/64-bit Citrix XenApp 6.0	Windows Server 2008 SP1/SP2 64-bit Edition with Terminal Server enabled, and with 32-bit/ 64-bit Citrix XenApp 5.0	Windows Server 2003 64-bit Edition with Terminal Server enabled, with 32-bit/64-bit Citrix XenApp 5.0/4.5 (formerly Presentation Server 4.5)	Windows Server 2008 R2 (Hyper-V)	Citrix XenApp 5.x/6.x XenDesktop 5.x/6.x	VMware View (VDI) 3.0, 3.1' 4.x	Windows 2003 Terminal Services (any SP level)	Windows 2000 Terminal Services (any SP level)	Citrix MetaFrame XP Server (any feature release, any SP level, Win 2000 and Win 2003)	Citrix MetaFrame PS 3.0 and 4.0 Enterprise Edition (*), (Win 2000 and Win 2003)/Advanced Edition, (Win 2000 and Win 2003)
Desktop and Process Analytics (DPA) Client	✓ **		✓ **	✓	✓	✓	✓			
DPA Process Discovery	✓ **		✓ **	✓	✓	✓	✓			

* Excluding support for the Citrix's Virtual Memory Optimization feature; the system must be added to the exclusion list of this feature. See Appendix A "Working with the Screen Capture Module" for further information on the Screen Capture Module and "Supported Terminal Server Sessions" on page 108.

** The DPA client for Citrix and Terminal Servers supports 64-bit operating systems. When capturing screens in this environment, the following are **not supported**:

- Capturing screens with embedded Internet Explorer browsers
- Capturing screens using web accessibility option
- Capturing screens using Dynamic Tables
- Capturing screens using Table column / Table Row feature

Hardware Specifications

The following table lists the hardware requirements for the workstations, per user role and per application where relevant:

	Agents	Supervisor Manager Admins	Forecasting and Scheduling
Disk Space			
For Desktop and Process Analytics: 10 MB for the client installation files and 100 MB to ensure processes run when there is no network. **For Real Time Speech Calibration Application:** 30 MBs per 100 media files for the temporary storage of media files that are played back during the validation and calibration process.	✓	✓	
Processor Speed			

	Agents	**Supervisor Manager Admins**	**Forecasting and Scheduling**
For Forecasting & Scheduling: Minimum: 1 Gigahertz (GHz). Recommended: 2 Gigahertz (GHz). For large enterprises with more than 2000 employees (and/or 100 queues) 3 Gigahertz (GHz).			✓
For Desktop and Process Analytics: Minimum: 1 Gigahertz (GHz). Recommended: 2 Gigahertz (GHz)	✓	✓	
Memory			
For Forecasting & Scheduling: Minimum: 1 GB. Recommended: 2 GB. For large enterprises with more than 2000 employees (and/or 100 queues) 4 GB.			✓
For Desktop and Process Analytics: Minimum: 1 GB. Recommended: 2 GB	✓	✓	
Monitor			
1024 x 768 high color - 16 bit	✓	✓	
For Forecasting & Scheduling and DPA Process Discovery: Recommended: 1280 x 1024			✓
For Speech Analytics: Recommended: 1280 x 1024		✓	
Sound/Video Cards			
Sound card + speakers and/or headphones		✓	✓
Peripherals			
Keyboard, Mouse, CD-ROM drive (or access to a shared network drive).	✓	✓	✓
Network			
10.100 Mbps 10-BaseT LAN Card	✓	✓	✓

Internet Explorer

Internet Explorer Supported Versions

The following web browsers are supported:

- Internet Explorer 9.0 32-bit
- Internet Explorer 8.0 32-bit
- Internet Explorer 7.0 32-bit

Internet Explorer Settings

The following browser settings are required for workstations installed with Playback or have access the Portal.

1 Open Microsoft Internet Explorer and select **Tools>Internet Options.**

2 Configure the **General** tab as follows:

- In **Browsing history**>**Settings>Temporary Internet Files>Check for newer versions of stored pages:**

  Select **Automatically** or **Every time I visit the webpage** (this option causes network overhead).

  Do not select Every time you start Internet Explorer or Never.

- In **Tabs**>**Settings**>**When a pop-up is encountered:**

  Select **Always open pop-ups in a new window**.

3 Configure the following **Security** settings for the web content zone**:**

The web content zone is based on network topology. For communication between the Desktop Application and the servers, the following servers and server roles are **required to reside in the same web content zone**:

- Application Server (or Load Balancer)
- Content Server role
- Framework Reports Server role

TIP Resolve the HTTP/HTTPS aliases from the Enterprise Management server settings or from the Site Preparation Checklist.

Otherwise, the Portal URL can reside in any zone, providing the zone is configured with the following security settings:

a. Select the relevant zone and in **Security level for this zone** click **Custom level....**

   The Security Settings dialog box for the zone appears.

b. Scroll down to **ActiveX controls and plug-ins** and set the following:
   - **Binary and script behaviors:** Set as **Enable.**
   - **Download signed ActiveX controls:** Set as **Enable** or **Prompt.**
   - **Run ActiveX controls and plug-ins:** Set as **Enable** or **Prompt.**
   - **Script ActiveX controls marked safe for scripting*:** Set as **Enable** or **Prompt.**

c. Scroll down to **Downloads** and set the following:
   - **File download:** Set as **Enable**. If the value selected is Disable, the desktop application installation method is limited to manually installing from the media. In addition, call forwarding in the Interactions Portal fails.

d. Scroll down to **Miscellaneous** and set the following:
   - **Access data sources across domains:** Set as **Enable**. If the value selected is Disable, Real-Time Monitoring does not function properly.
   - **Allow script-initiated windows without size or position constraints:** Set as **Enable**.
   - For Ad-hoc Reporting, set **Submit non-encrypted form data** to **Enable**.

e. Scroll down to **Scripting** and set the following:
   - **Active scripting:** Set as **Enable** or **Prompt**.
   - **Allow Programmatic clipboard access:** Set as **Enable**.
   - **Scripting of Java applets:** Set as **Enable** or **Prompt**. If the value selected is Disable, the Data Analytics Instance Builder may not function properly.

f. Scroll down to **User Authentication** and set the following:
   - For Windows Desktop **Single-Sign On (SSO)**, the web content zone of the servers and server roles communicating with the workstation must be set to **Automatic logon only in Intranet zone** (for local intranet or trusted zones) or **Automatic logon with current username and password** (internet zone).

g. Click **OK** to return to the Internet Settings window.

h. If logging is required, disable Protected Mode (relevant for Windows Vista and later OS; not supported in Windows XP):

   i. Below the **Security level for this zone** area, and directly above the **Custom level...** and **Default level** buttons, clear the **Enable Protected Mode** option.

   ii. Click **OK** on the Internet Options window.

   iii. If you're prompted with a **Warning!** dialog box, advising that **The current security settings will put your computer at risk,** click the **OK** button.

   iv. Close Internet Explorer and then open it up again.

4. Configure the **Advanced** tab as follows:

   For Application Authentication>Windows Authentication (Active Directory)>Single Sign-On (SSO):

   - Scroll to **Security** and select **Enable Integrated Windows Authentication* (requires restart)**.

   For workstations accessing the **Data Analytics** Application:

   - For users with rights to access the Data Analytics Instance Builder application, scroll to **Java (SUN)** and select check **Use JRE 1.5/1.6<any update level> for <applet>**. This parameter appears after the Instance Builder application is installed.
   - For exporting Data Analytics Instances in SSL environments, scroll to **Security** and clear **Do not save encrypted pages to disk**.

   For workstations accessing **Ad-Hoc Reporting:**

   - Scroll to **Printing** and select **Print background colors and images**.

   For DPA 64-bit Citrix client:

   - Scroll to **Browsing** and select **Enable third party browser extensions * (requires restart)**.

     This is required for installing two add-ons for the DPA client. Make sure not to disable these add-ons after installation.

5. Configure the **Privacy** tab as following:

   a. In **Settings,** set Select a setting for the Internet zone to **Medium**, **Low**, or **Accept All Cookies**.

   b. click **Advanced** and clear **Override automatic cookie handling** and click **OK** to return to the Privacy tab.

   c. In **Pop-up Blocker** click **Settings**. In **Address of Web Site to Allow** enter the Portal address and click **Add**. The address appears in the Allowed Sites box.

Third Party Software

- Third Party Software Required by Desktop Applications, page 23
- Third Party Software Required for Browsing, page 24

Third Party Software Required by Desktop Applications

The following table lists the **minimum 3rd party software requirements** for each Desktop Application installed on the end user machines.

	Microsoft MSchart	Microsoft Windows Installer 3.1 or later	Microsoft Data Access Components (MDAC) 2.8 SP2	Microsoft .NET Framework 2.0 SP1	Microsoft .NET Framework 3.5	Microsoft Visual C++ 2008 Runtime 32-bit**	Microsoft Visual C++ 2005 Runtime	Microsoft WSE Runtime 2.0 SP3	Microsoft® DirectX® 9	MSXML 4.0 SP3	Adobe® Flash® Player Plugin version 7 or later	JRE 1.4.2 uses Access Bridge 1.2 or 2.0 ***	Microsoft Message Queue (MSMQ)
Screen Capture Module (including AIM)		✓											
Playback		✓				✓			✓	✓			
Form Designer		✓	✓	✓									
Standalone Form Designer		✓	✓		✓								
User Import Support Package		✓											
Logger		✓		✓		✓							
Pop-up Notification System Client		✓		✓									
Content Producer				*		*			✓	*	✓		
Forecasting and Scheduling		✓											
Strategic Planner		✓											
Phonetics Boosting	✓			✓									
Real Time Speech Calibration Application				✓									
Desktop Resources		✓		✓									
Desktop Gadgets					✓								
Desktop and Process Analytics (DPA) Client												✓	****
DPA Process Discovery	✓				✓								

* Required in order to produce Interactions clips.

** When running Windows 64-bit Operating Systems, note that Microsoft Visual C++ 2008 Runtime 32-bit is required.

*** If a customer's third party software requires a specific legacy Java environment, the Java access bridge version for this legacy Java environment must be installed. For details, see http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html.

**** MSMQ is required for the 64-bit Citrix or Terminal Server version of the DPA Client only. The MSMQ Server and MSMQ Server core features are required.

Third Party Software Required for Browsing

The following lists the prerequisite software required to enable workstation users to browse to the web based applications:

Software	Web Based Application
Adobe Flash Player Plugin Version: 7 and higher	Required for Trend Analysis performed in **Speech Analytics** applications.
Java Runtime Environment (JRE) Version: JRE 5.0, JRE 6.0, JRE 7.0 are supported including all minor version releases. The recommended versions are JRE 7.0 update 2, JRE 6.0 update 14, and JRE 5.0 update 18.	The following web client applications require JRE: ● **Data Analytics** Instance Builder ● Storage Manager Rule Editor used by **Speech Analytics** ● **Strategic Planner** uses JRE version 6 or above ● **WFM** packages using Pulse, Adherence, Calendar, Forecasting & Scheduling use JRE version 6 or above ● **Ad-Hoc Reporting**
Windows Media Player Version: 9 and higher	● 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. ● Required for playback controls in the **Real Time Speech Calibration Application**.

Software Dependencies

Software Dependencies between Desktop Applications

The following table lists the desktop applications, that as a prerequisite, require other desktop applications to be installed.

	Desktop Resources	**Multimedia Support Package or Playback**
Screen Capture Module (including AIM)		
Playback	✓	
Form Designer	✓	
Standalone Form Designer	✓	
Logger	✓	
Pop-up Notification System Client		
Content Producer		*
Forecasting and Scheduling		
Strategic Planner		
Phonetics Boosting	✓	
Real Time Speech Calibration Application	✓	✓
Desktop Gadgets		
Desktop and Process Analytics (DPA) Client		
DPA Process Discovery		

* Required in order to produce Interactions clips.

Software for Desktop and Process Analytics (DPA)

This section list the third-party software required for DPA triggering and analysis using Process Discovery.

Software for DPA Clients

DPA uses Java Access Bridge when DPA triggers are required on Java based applications and are configured to capture screen controls within of the Java applet.

- Java Access Bridge 1.2 for JRE 1.4 or Lower
- Java Access Bridge 2.0.2 for JRE 1.5 or above

Software for Process Discovery Clients

When not detected on the desktop, these items are installed automatically by the clients.

- **Microsoft Visio:** Version 2007, 2010
- **Microsoft Office Primary Interop Assemblies**: Version 2007
- **Visual Studio Tools for Office Runtime**: Version VSTO 2005.

Localization

The Desktop Applications support localized customers. The following table indicates the localization languages supported and if double-byte languages are supported, per Desktop Applications.

Desktop Applications support localization of more than one language simultaneously.

Desktop Application	Support for Double-Byte Languages	Supported GUI Languages
Browsing to Web Clients from Workstation:		
Browsing to the Portal	✓	
Browsing to Customer Feedback application	✗	
Desktop Applications:		
Screen Recording (including AIM)	✓	Localization is not supported
Pop-up Notification System Client Forecasting and Scheduling Strategic Planner	✓	Chinese (Simplified) French German Japanese Portuguese (Brazilian) Russian Spanish Dutch
Content Producer	✓	Localization is not supported

Desktop Application	Support for Double-Byte Languages	Supported GUI Languages
Playback Form Designer Standalone Form Designer User Import Support Package Logger	✓	Chinese (Simplified) French German Japanese Portuguese (Brazilian) Russian Spanish Hebrew Dutch
Real Time Speech Calibration Applications	✓	Localization is not supported
DPA Desktop Prompts	✓	Japanese
Desktop Gadgets	✓	Chinese (Simplified) French German Japanese Portuguese (Brazilian) Russian Spanish Dutch

CTI Link Agent and Localized Systems

This section is only relevant for systems with Acquisition Recording.

- When **Interactive Agent Login is enabled**, Agents must login in English. This is required when agents do not have unique credentials and CTI Link does not provide agent identification.
- When **Interactive Agent Login is disabled**, localized agent login is supported as agents log in using their Windows credentials.

Set Windows Regional and Language Settings

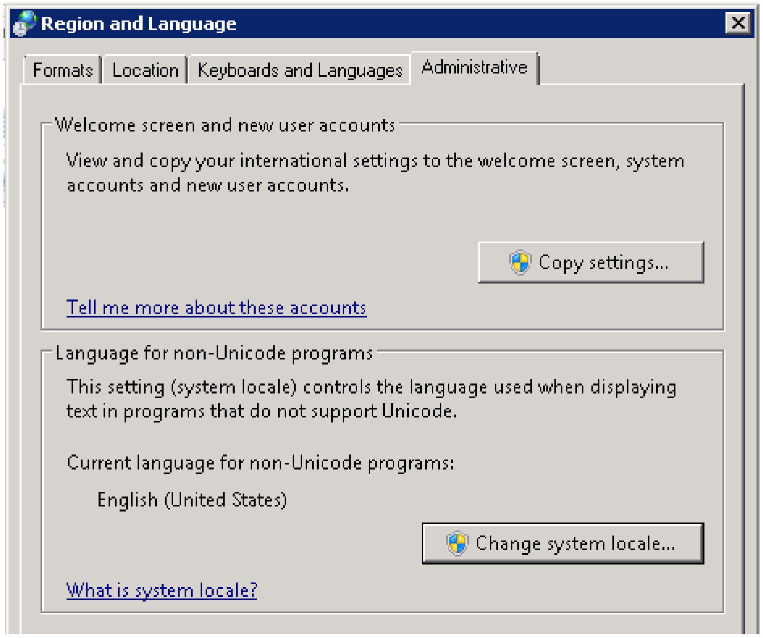
Windows regional settings *must* be set in their local language (not English) to provide localized support for Playback and to view Record On-Demand in a language other than English.

Define the format, location and language for non-Unicode programs:

1 From the **Control Panel** select **Regional and Language Options**.

The Regional and Language Options screen is displayed.

2. **Define Format:** Format defines the locale to use for the display of the date, time, currency, and measurements:
3. **Define Location:** Location indicates the country or region that you are in.
4. **Define Language for non-Unicode programs** (system locale). This determines the default character set (letters, symbols, and numbers) and font that you use to enter information and that are used to display information in programs that do not use Unicode. This allows non-Unicode programs to run on your computer using the specified language:



View and copy your international settings to the welcome screen, system accounts and new user accounts.

This setting (system locale) controls the language used when displaying text in programs that do not support Unicode.

Current language for non-Unicode programs:

English (United States)

5. **Supporting East Asian Languages:**
   - **Windows XP and Server 2003:** Include native support for East Asian languages. To install the files, check the Install files for East Asian languages in the Control Panel > Regional and Language Options > Languages. Note that a minimum of 230 MB of disk space is required and that the Windows CD-ROM is needed.
   - **Windows Vista and 7:** Include support for East Asian characters in the standard installation.

Set Browser Language Settings

Dates and calendars are displayed in local format. The system handles dates in Greenwich Mean Time (GMT) in the database, then shows them according to the locale and language for which your system is configured.

Language settings should be set to reflect the user interface language.

To change your browser language settings and display dates in local format:

1. Select **Internet Options** from the **Tools** Menu in Internet Explorer.
2. Select the **Languages**... button from the General tab.
3. Set your language preference.

   If your operating system is Windows XP, you also need to install the corresponding language pack.
4. On the browser of the client machine:

   a. Select **Encoding** from the View menu.

   b. Select **Unicode (UTF-8)**.

Chapter 3

Installation by Role: Silent Distribution

Silent Distribution Guidelines

Silent distribution is used to batch install multiple desktop applications on the end user machines. 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 distributed 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 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.

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:

      i. Select **Share this folder**.

      ii. Click **Permissions.**

      iii. 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 application(s) without requiring user intervention.

The workflow for distributing the application(s) silently, is as follows:

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, gadgets (if relevant), and logging for troubleshooting purposes.

- Desktop Applications for Agents, page 33
- Example Script for Agents, page 33

Desktop Applications for Agents

The following Desktop Applications are required for users defined as Agents:

- Desktop Resources (prerequisite for Logger)
- Screen Capture and AIM
- Desktop Gadget
- Logger
- Desktop and Process Analytics (DPA) Client: Installed separately as part of a DPA deployment. The installation instructions are in the *Desktop and Process Analytics (DPA) Installation and Configuration Guide*.

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

Example Script for Agents

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

```
@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:>\Impact360_DesktopApplications
set INSTALLFOLDER=C:\Program Files\<Company Name>
SET EXIT_CODE=0

echo Desktop Resources Installation
msiexec -i "%MSIS_DIR%\DesktopResourcesVerint.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 Gadgets
msiexec /i Gadget.msi /qn INSTALLDIR="%INSTALLFOLDER% SERVER_URL=<NLBName>
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%
```

Silent Distribution for Supervisors/Manager

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.

- Desktop Applications for Supervisors/Managers, page 35
- Example Script for Supervisor/Manager, page 35

Desktop Applications for Supervisors/Managers

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

- Desktop Resources (prerequisite for Playback and Logger)
- Playback
- Forecasting and Scheduling
- Strategic Planner
- Logger
- Desktop Gadgets

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

For Supervisors or Managers that are given Administrator privileges and are required to design Forms, include the Form Designer in the example script.

Example Script for Supervisor/Manager

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

```
@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:>\Impact360_DesktopApplications
set INSTALLFOLDER=C:\Program Files\<Company Name>
SET EXIT_CODE=0

echo Desktop Resources Installation
msiexec -i "%MSIS_DIR%\DesktopResourcesVerint.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%" PLAYBACK_ENCRYPTED=0 ADDLOCAL=Playback NOREBOOT=1 /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
 echo ---installer failed
)  ELSE  (
echo ---installer succeeded
)

echo Gadgets
msiexec /i Gadget.msi /qn /l*vx "c:\gadget.log" INSTALLDIR="%INSTALLFOLDER% "Remove /l*vx
"c:\gadjet.log" SERVER_URL=<NLBName>
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
)  ELSE    (
echo ---installer succeeded
)

echo Forecasting and Scheduling Installation
msiexec -i "%MSIS_DIR%\ForecastingandScheduling.msi" USE_COMMAND_LINE=1
INSTALLDIR="%INSTALLFOLDER%" SZAPPSERVERNAME=<NLBName> SZAPPSERVERPORT=7001 /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
)  ELSE  (
echo ---installer succeeded
)

echo Strategic Planner Installation
msiexec -i "%MSIS_DIR%\Setup.exe " USE_COMMAND_LINE=1 INSTALLFOLDER="%INSTALLFOLDER%" /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%
```

Silent Distribution for Administrators and Analysts

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

- Desktop Applications for Administrators and Analysts, page 37
- Example Script for Administrators and Analysts, page 37

Desktop Applications for Administrators and Analysts

The Desktop Applications required for users defined as Administrators are listed here.

- Desktop Resources (prerequisite for Playback, Form Designer, Real Time Speech Calibration Application, and Phonetics Boosting)
- Playback
- Form Designer
- User Import Support Package
- Logger
- Real Time Speech Calibration Notification: Used by Analysts with an understanding of the enterprise requirements for Real Time Speech Notifications.
- Phonetics Boosting: Used by Speech Analytics analysts. Does not support silent installation.
- DPA Process Discovery: Installed separately as part of a DPA deployment. The installation instructions are in the *Desktop and Process Analytics (DPA) Installation and Configuration Guide*.

Example Script for Administrators and Analysts

This script is an example for silently installing the desktop applications for the predefined agent role. 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" on page 37.

```
@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:>\Impact360_DesktopApplications
set INSTALLFOLDER=C:\Program Files\<Company Name>
SET EXIT_CODE=0
```

```
echo Desktop Resources Installation
msiexec -i "%MSIS_DIR%\DesktopResourcesVerint.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=NLBName GLOBAL_USE_SSL=0
GLOBAL_APP_SERVER_AUTH_PORT=<80>/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%" PLAYBACK_ENCRYPTED=0 ADDLOCAL=Playback NOREBOOT=1 /qn
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
)
```

```
echo Real Time Speech Calibration Application Installation
msiexec /i Real Time Speech Validation Application.msi  /quiet INSTALLROOT="%INSTALLFOLDER%"
GLOBAL_APP_SERVER_DNS="NLBName" GLOBAL_USE_SSL="NO"  USE_COMMAND_LINE=1 WFO_PORT=7001



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%
```

Chapter 4

Installation by Application

Content Producer

Content Producer Overview

Content Producer is installed and used as a standalone product.

Content Producer is comprised of authoring, editing, and conversion tools to develop learning clips. If you use Content Producer with the suite, you can create clips from the recorded segments of customer interactions and then deliver the learning clips via the eLearning Lesson Management system.

Content producer has an authoring component to create/publish clips and an editor component to import/record audio or video contact files (.wav or .avi).

This chapter contains the information required to install Content Producer. For further information refer to the following documents:

- *Content Producer User Guide*

All site preparation and system requirements must be met before starting the installation. See Chapter 2 “Customer Requirements”.

- **Hardware Requirements**
  - Intel PIII/AMD K6 550 MHz. For optimal performance, the following is recommended: Intel P4, Intel Centrino, Intel Xeon, or Intel Core Duo (or compatible)
  - 512+ MB RAM (1GB Recommended for optimal performance)
  - 16 Bit+ Video card - 800x600 minimum resolution (1024x768 recommended)
  - 5+ GB Hard Drive with 500+ MB free disk space
- **Content Producer installation file:** Available from the Portal’s Tools folder.
- **License code:** Required to activate Content Producer after installation. You will receive the Content Producer license code with your fulfillment package.
- **Internet access:** For registering Content Producer and upgrading to newer versions.
- **Playback:** Required in order to produce clips of interactions. See “Playback” on page 63.

NOTE If you have the Multimedia Support Package (Playback) 9.3 application installed on your system, uninstall the application before starting the Content Producer installation. If you do not uninstall this package, you will be prompted during the Content Producer installation to remove it before continuing with the installation.

- **Media Formats Supported:**
  - Content Producer Author supports the following formats: JPG, GIF, TIFF, BMP, PNG, MP3, AIFF, AU, SWF (Created in Adobe® Flash® Editor version 8 or earlier)
  - Content Producer Editor supports the following formats: AVI, WAV

Manually Installing Content Producer

Manual installation is the only supported installation method.

1 Double-click the **ContentProducer11.1.0.exe** file.

The first window in the Installation Wizard is displayed.

2 Click **Next**.

The **License Agreement** screen is displayed.

3 On the **License Agreement** screen, click **I accept the agreement** option, and then click **Next**.

The **Select Destination Directory** screen is displayed.

4 If you want to change the default destination, click the **Browse** button, navigate to and then select another directory in which you want to store the program files. Click **Next**.

The **Select My Clips Directory** screen is displayed.

5 If you want to change the default destination for clip files generated by Content Producer, navigate to and select another directory. Click **Next**.

The **Enter the URL for the Impact 360** screen is displayed.

6 If you want to configure Content Producer to automatically populate lesson information on the eLearning Lesson Details page, type the URL for the system suite. Click **Next**.

NOTE After Desktop Applications is installed, you can add or modify the system suite URL in Content Producer Author. Click **Edit** > **Preference** > **Advanced**.

The Select Start Menu Folder screen opens.

7 If you want to change the default Start Menu folder in which Content Producer’s shortcuts are saved, select a folder from the list box. Click Next.

The File Associations screen opens.

8 Click **Next**.

The **Select Additional Tasks** screen opens.

9 Click **Next**.

The installation process begins, and its progress is displayed on the **Installing** screen. When the process is complete, click **Finish** to end the installation.

NOTE If your system has the Multimedia Support Package 9.3 application installed, a warning message appears during the installation to indicate that you must first uninstall this application before resuming your installation.

Once the installation is complete, shortcuts for Content Producer components appear on your desktop, as follows:

- ✓ Content Producer Author
- ☑ Content Producer Editor

You can also access Content Producer components by clicking **Start > Content Producer**.

10 To activate your license, see "Activating and Registering Your License" on page 44**.**

Installing Microsoft DirectX

If Content Producer detects you do not have Microsoft DirectX installed or your system requires an updated version of DirectX, the **Welcome to setup for DirectX** screen opens:

NOTE If, during the course of the installation, Content Producer detects that you do not have Microsoft DirectX installed, you are prompted to install the Microsoft DirectX. For details, see "Installing Microsoft DirectX" on page 43.

To install Microsoft DirectX

1 Click the **I accept the agreement** button to confirm you accept the terms of the licensing agreement, and then click **Next**.

The **Installing Microsoft DirectX** screen opens, indicating that components are downloading, and showing the time left for the process to complete. It may take several minutes.

2 When the process is complete, click **Next** to open the **Restart Computer** screen.

3 When you are ready to restart your computer, click **Finish**.

Activating and Registering Your License

Once you install Content Producer, you need to activate and register your license.

If you are activating and registering your license on a desktop...	See...
With an Internet connection	"Activating and Registering a License on a Desktop with an Internet Connection" on page 44.
Without an Internet connection	"Activating and Registering a License on a Desktop without an Internet Connection" on page 45.

NOTE If you are accessing the Internet using a proxy server, you need to set proxy server preferences first, so that you can activate your license, receive updates, and access Content Producer Help and support site. For details, see Step 5 in the procedure "Setting Preferences in Content Producer" on page 45.

Activating and Registering a License on a Desktop with an Internet Connection

1 Click **Start > Content Producer > Content Producer Author**.

The Content Producer main window opens.

2 In the left pane, select **License Activation**.

The **License Activation** dialog box opens.

3 In the **License Code** box, type the license code that you received, and then click **Next**. If you entered the code correctly, the **Registration** dialog box opens.

4 Type the appropriate details in the dialog box, and then click **Next**.

A progress screen appears, and if the activation is successful, the screen refreshes with the **Successful** dialog box.

5 Click **Finish** to complete the process and close the dialog box.

In the Content Producer main window, in the **Help** area, **Licensed** appears under the **License Deactivation** item. You are now ready to use Content Producer.

NOTE If the license activation process is not successful, though you entered the correct license key, contact your support consultant.

6 To configure Content Producer by setting preferences, see "Setting Preferences in Content Producer" on page 45.

Activating and Registering a License on a Desktop without an Internet Connection

1 Follow steps 1 to 4 in the procedure "Activating and Registering a License on a Desktop with an Internet Connection" on page 44.

Because your desktop does not have an Internet connection, the **Connection Problem** window is displayed.

2 Click the **Web Activation** link.

The **Web Activation** window is displayed.

3 From the **Step 1: Open the Web Activation Web** page box, copy the URL address.

NOTE Because you do not have an Internet connection, copy the URL address to a text file, and save the file to a disk. Insert the disk and open the file on a desktop that has an Internet connection, and from the text file, copy the URL address again.

4 At a desktop that has an Internet connection, open a web browser, and paste the URL into the browser's address box. Click **ENTER**.

The online **Web Activation** screen opens.

5 Click **Submit**.

The **Web Activation** screen refreshes, showing the confirmation code in the **Confirmation Code** box.

6 Copy the confirmation code, using the same method you used in step 3 (for example, by copying it to a text file and saving it to disk), and then close the page.

7 Return to the desktop without an Internet connection for which you are activating and registering the license. In the **Web Activation dialog** box, paste the confirmation code from step 6 into the **Step 3: Enter the supplied Confirmation Code** text box.

8 Click **Next**.

The confirmation code is verified, and your license is activated. You can begin using Content Producer.

9 To configure Content Producer by setting preferences, see "Setting Preferences in Content Producer" on page 45.

Setting Preferences in Content Producer

1 Launch Content Producer by clicking the Content Producer Author icon ✓ on your desktop, or by clicking **Start > Content Producer > Content Producer Author**.

2 On the menu bar of the Content Producer main window, click **Edit > Preferences**.

The **Preferences** dialog box opens.

3 To set recording countdown timing preferences, click the **General** tab. Make the changes you want in the **Recording** areas of the tab.

4 To choose a dictionary and spelling preferences (such as whether or not to check for upper and lowercase words), click the **Spelling** tab. Make changes as required.

5 If you access the Internet with a proxy server, you must set proxy server preferences so that you can activate your license, receive Content Producer updates, and access the Help files and the support site. Click the **Proxy** tab and do the following:

- Check the **Use a proxy server** box
- Enter the proxy server's IP address and port number in the **Address** and **Port** boxes.

NOTE Ensure that you type the proxy servers' IP address, not a URL address, in the **Address** box.

- If the server requires login authentication, check the **User proxy authentication** box, and type the login name and password in the **Login** and **Password** boxes.

6 To create log files that record issues that arise while you are using Content Producer, click the **Logging** tab, and do the following:

- In the **Output Window** area, select a logging option from the **Report** drop-down list box.

For...	Select...
normal day-to-day application use	**Display Errors Only** This option only logs application error events.
troubleshooting issues	**Display All Information** This option logs all application event types including information events for successful operations. It impacts application performance.

- In the **Log File** area, select the options for outputting log records to a file.

7 To enable backup file options, click the **Backup** tab.

8 To change Java virtual machine settings, click the **Advanced** tab.

9 Click **OK** to save your preferences and close the dialog box.

Upgrading Content Producer

Once you have installed Content Producer, you find out about and upgrade to new releases. This section contains the following information:

Checking For and Upgrading to the Most Recent Content Producer Release

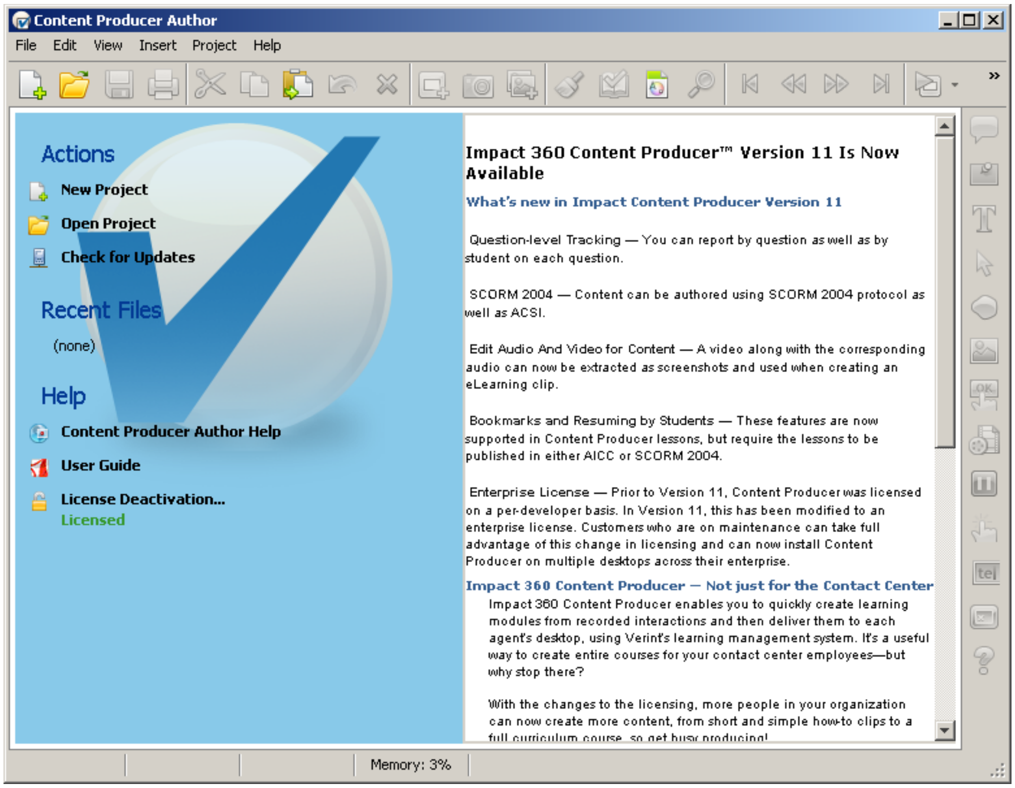
You can check for the latest Content Producer release from the Content Producer Author Welcome window.

Note that if your company’s firewall prevents automatic registration or updates, you must first configure the appropriate proxy information, as described in step Step 5 in the procedure “Setting Preferences in Content Producer” on page 45.

To successfully upgrade to the most recent Content Producer release, see “Checking for and Upgrading to the Most Recent Content Producer Release” on page 47.

Checking for and Upgrading to the Most Recent Content Producer Release

1 Launch Content Producer to open the **Welcome to Producer** window.



Impact 360 Content Producer™ Version 11 Is Now Available

What’s new in Impact Content Producer Version 11

Question-level Tracking — You can report by question as well as by student on each question.

SCORM 2004 — Content can be authored using SCORM 2004 protocol as well as ACSI.

Edit Audio And Video for Content — A video along with the corresponding audio can now be extracted as screenshots and used when creating an eLearning clip.

Bookmarks and Resuming by Students — These features are now supported in Content Producer lessons, but require the lessons to be published in either AICC or SCORM 2004.

Enterprise License — Prior to Version 11, Content Producer was licensed on a per-developer basis. In Version 11, this has been modified to an enterprise license. Customers who are on maintenance can take full advantage of this change in licensing and can now install Content Producer on multiple desktops across their enterprise.

Impact 360 Content Producer — Not just for the Contact Center

Impact 360 Content Producer enables you to quickly create learning modules from recorded interactions and then deliver them to each agent’s desktop, using Verint’s learning management system. It’s a useful way to create entire courses for your contact center employees—but why stop there?

With the changes to the licensing, more people in your organization can now create more content, from short and simple how-to clips to a full curriculum course, so get busy producing!

2 In the **Actions** area, click **Check for Updates**.

The **Check for Updates** dialog opens.

3 Choose one of these options:

- Select the **Content Producer automatically check for updates** option, and from the drop-down list box, select the time interval within which you want the system to check for updates: **Daily**, **Weekly**, or **Monthly**. The default is **Weekly**.

- Select the **Manually check for updates** option. Choosing this option prohibits the system from automatically checking for updates.

4 To immediately check for updates, click **Check Now** then click **OK**.

5 You either get a message with information about updates, or a message that your version of Producer is up-to-date.

NOTE During an upgrade, the **My Documents\My Clip Assets Library** folder is renamed, such that a number which includes the date of the upgrade is attached to the folder name (for example, the new name of the old folder might be: **My Clip Assets_Library_11.1.3010_20110802**).

If you created your own HTML frame template in the previous version of Content Producer, you can retrieve your template from this folder. Because the HTML frames are changed in the new release, the best practice is to customize your HTML frames using the latest version’s templates.

Upgrading From Pre-7.8.x Versions of Content Producer

1 Click **Start > Settings > Control Panel > Add or Remove Programs**.

2 In the **Add or Remove Programs** window, locate the pre-7.8.x version of Producer that you want to remove, and select it.

3 Click **Remove**.

Once the uninstall process ends, the pre-7.8.x version of Producer is removed from your system.

4 Install the new release of Content Producer, as described in the procedure “All site preparation and system requirements must be met before starting the installation. See Chapter 2 “Customer Requirements”.” on page 41.

Desktop Gadget

Desktop Gadget Overview

The Desktop Gadget provides employees with their KPI information on their desktop where they can easily glance at it throughout their shift. Providing this important information on their desktop makes it easy for employees to be aware of their performance and gives them the opportunity to make adjustments when necessary to meet their goals.

The information provided on the KPI Gadget varies based on the licenses your company has purchased and how the gadget is configured (that is, the selected options and the KPI periodicity).

The KPI Gadget feature is especially useful with Intraday KPIs. It shows near real-time data to employees as they work. However, if your organization does not have the licenses required for Intraday KPIs, you can still create KPI Gadgets for the other periodicities (such as Daily, Weekly).

This chapter contains the information required to install the gadget. For further information regarding configuration and usage of the gadget, refer to the following documents:

- *Scorecards Administration Guide*
- *Scorecards User Guide*

All site preparation and system requirements must be met before starting the installation. See Chapter 2 “Customer Requirements”.

Manually Installing Desktop Gadget

The Desktop Gadget manual installation procedure must be performed on the desktop on which the application will be run.

To install the Desktop Gadget:

1. Double-click the **Gadget.msi** to launch the Installation Wizard.
2. Click **Next** and read the End-User License Agreement.
3. Select **I accept the terms in the license agreement** and click **Next**.
4. In the **Destination Folder** window, click Next to install to the default folder, or click Change to install to a different folder.
5. In the **Server URL** window enter the **name of the server** associated with the Framework Application Server Role or Load Balancer. If not configured during installation, the user is asked to enter the address when first opening the application.

6 In the **Ready to Install** the Program window, click **Install** to begin the installation.

7 The **Installing Desktop Gadget** window appears displaying the installation status.

8 When the installation is complete, the **InstallShield Wizard Completed** window appears. Click Finish. Click **Finish**. The Desktop Gadget icon appears on the desktop.

In addition the gadget can be initiated from the start menu or from...**Program Files\<Company Name>\Desktop Gadgets**. Following initialization a tray icon is used to control the gadget and change the configuration settings.

Desktop Gadget Silent Install Parameters

The Desktop Gadget is installed on Agent desktops. Refer to Chapter 3 “Installation by Role: Silent Distribution” for a sample script that includes the command line for distributing this application in silent mode.

The following properties determine how the Desktop Gadget is configured silently on the agent desktops.

Parameters	Description and Default Values
MsiFIle	Gadget.msi
USE_COMMAND_LINE	USE_COMMAND_LINE=1 **Mandatory**
<log file path>	The path to the gadget log files Default is C:\gadget.log
INSTALLDIR	Specifies the installation destination Default is C:\Program Files\<Company Name>\Gadget
SERVER_URL	Name of the Application Server or Load Balancer. **Default=Empty**

Desktop Resources

Desktop Resources Overview

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

For a complete list of the desktop applications dependent on Desktop Resources, refer to "Software Dependencies" on page 25.

For all software and hardware specifications refer to Chapter 2 "Customer Requirements".

Manually Installing Desktop Resources

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

To install Desktop Resources:

1 Double-click the **DekstopResources.msi** to launch the Setup Wizard.

2 If a security warning appears, click **Run**.

The installer asks you to wait while it configures the Desktop Resources, and closes automatically.

- Desktop Resources is now listed in Add/Remove Programs
- The Registry now contains the brand related keys here: HKEY_LOCAL_MACHINE>SOFTWARE>IMPATCT360>INSTALL

Desktop Resources Silent Install Parameters

The following properties determine how Desktop Resources is installed silently on the desktops. Refer to Chapter 3 "Installation by Role: Silent Distribution" for a sample script that includes the command line for distributing this application in silent mode.

Parameters	Description and Default Values
MSIS_DIR	<Shared network folder:>\Impact360_DesktopApplications
MsiFIle	DesktopResourcesVerint.msi

Parameters	Description and Default Values
USE_COMMAND_LINE	USE_COMMAND_LINE=1 **Mandatory**
TARGETDIR	Specifies the installation destination

Desktop and Process Analytics (DPA) Client

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

Installed separately as part of a DPA deployment, the DPA client installation instructions are documented in the *Desktop and Process Analytics (DPA) Installation and Configuration Guide*.

DPA Process Discovery

Visio based reporting tool for DPA Analysts. Process Discovery provides a means to discover workflow variations between users and to visualize these workflows as Microsoft Visio diagrams.

Installed separately as part of a DPA deployment, the DPA Process Discovery installation instructions are documented in the *Desktop and Process Analytics (DPA) Installation and Configuration Guide*.

Forecasting and Scheduling Client

Forecasting and Scheduling Installation Overview

Forecasting and Scheduling provides a Supervisor or Manager with an intuitive desktop solution for managing and planning contact center activities including:

- Flexible forecasting and scheduling based on your contact center rules and needs.
- Virtual contact center management.
- Seamless integration with your automated call distributor (ACD).
- Queue- and group-level performance analysis and monitoring with easy-to-read graphs.
- Robust employee management tools.

For all software and hardware specifications refer to Chapter 2 "Customer Requirements".

Manually Installing Forecasting and Scheduling

Installing Forecasting and Scheduling

1. Run the **ForecastingandScheduling.msi** file.
2. In the Welcome screen, click **Next**.
3. In the License Agreement screen, select **I 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. In the Configuration screen, type the **Application Server** name or Load Balancer name, and **Port** that Forecasting and Scheduling connects to, and then click **Next**.

   NOTE The Port number is always HTTP port number 7001, including for SSL systems.

6. In the Ready to Install screen, click **Install**.

   When the installation is complete, the **Installation Success** window appears.

7 Click **Finish** to exit the installation wizard.

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

8 Restart your computer.

Installing Forecasting and Scheduling on Windows Vista

Due to how Windows Vista registers system DLLs and/or OCXs, the following steps must be taken to install Forecasting & Scheduling on Windows Vista.

1 Install Forecasting & Scheduling on Windows Vista using the **<DVDROOT>\SuiteCd4_ForecastingAndScheduling\ForecastingAndScheduling** path.

2 Open an Administrative DOS console and run **SetupForVista.cmd**.

When the installation window opens, follow Step 2 to Step 8 of the procedure described at "Installing Forecasting and Scheduling" on page 53.

Forecasting and Scheduling Silent Install Parameters

The following properties determine how Forecasting and Scheduling is configured silently Refer to Chapter 3 "Installation by Role: Silent Distribution" for a sample script that includes the command line for distributing this application in silent mode.

Parameters	**Description and Default Values**
MsiFIle	ForecastingandScheduling.msi
SZAPPSERVERNAME	The name of the server hosting the Framework Applications server role (the Application Server or Load Balancer). **Mandatory**.
SZAPPSERVERPORT	The port number of the Framework Applications server role (hosted on the Application Server or Load Balancer) **Default** =7001
INSTALLDIR	Specifies the installation destination **Default** = C:\Program Files\<company name>\Forecasting and Scheduling

Form Designer

Form Designer Overview

The Form Designer is used for designing evaluation and assessment forms.

This chapter contains the information required to install the Form Designer. For further information using Form Designer, refer to the following documents:

- *Quality Monitoring Form Designer User Guide*

For all software and hardware specifications refer to Chapter 2 “Customer Requirements”.

Manually Installing Form Designer

This application requires the mandatory resources contained in Desktop Resources. Ensure “Desktop Resources” on page 51 is installed on the desktop before proceeding.

1 Run the **FormDesignerInstallation.msi** file.

The **Welcome** screen of the setup wizard appears.

2 Click **Next**.

The **End-User License Agreement** screen appears.

3 Select **I accept the terms in the License Agreement** and click **Next**.

The **Custom Setup** screen appears.

To view the required space for an application, select it in the list and read the text in the pane on the right.

4 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** screen appears.

6 Enter the address of the Application Server or Load Balancer. If required, resolve the address as follows:

a. Access the Portal and Select the **System Management** tab.

b. Select **Enterprise Management > Enterprise Settings.**

c. Select the **Server Settings** tab of the Server associated with the Framework Applications Server Role.

d. Expand **Additional Settings** to find the HTTP/HTTP Alias.

7 Enter the **Port Number of the Framework Applications server role**. Refer to the *Firewall Ports Configuration* spreadsheet for details on the default port for SSL and non-SSL systems.

8 (Optional) Select **Use SSL for client/server communication**.

9 Click **Next**.

The **Ready to Install** window appears.

10 Click **Install**.

When the installation is complete, the **Installation Success** window appears.

11 Click **Finish** to exit the installation wizard.

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

12 Restart your computer.

Form Designer Silent Install Parameters

The following properties determine how Form Designer is silently configured. See Chapter 3 "Installation by Role: Silent Distribution" for a sample script that includes the command line for distributing this application in silent mode.

Parameters	Description and Default Values
MsiFIle	FormDesignerInstallation.msi
VERINTFOLDER	Specifies the installation destination
USE_COMMAND_LINE	USE_COMMAND_LINE=1 **Mandatory**
GLOBAL_APP_SERVER_DNS	Name of the Application Server or Load Balancer. **Mandatory**
GLOBAL_APP_SERVER_AUTH_PORT	The port number of the Framework Applications server role (authentication URL port, by default = 7001, or 7002 if SSL is configured). **Mandatory**
GLOBAL_USE_SSL	0 = Do not use SSL. 1 = Use SSL. **Default = 1**
TERMINAL_SERVER	0 = No Terminal server. 1 = Terminal server mode. **Default** = Auto detect.

Form Designer (Standalone)

This chapter provides instructions for installing the Form Designer as a Standalone application prior to installing the system. This is for customers that need to build forms prior to the system deployment.

This chapter includes:

Form Designer (Standalone) Overview

This Installation Guide provides instructions for installing the Form Designer as a Standalone application prior to installing the system.

Some of the functions described in the Form Designer online help and user guide are not available because this is a standalone application. The following functions are not available in the Standalone Form Designer:

- Shared components are not available.
- Shared data is not available. This includes Evaluations Custom Data (including auto population from any external source), Status 1 and Status 2, Rating, Reasons and Default Form.
- In the Form List window, the following menu buttons are disabled in the Form List toolbar: Open Form, Delete Form, Change Status, Export Form, Export to Excel, Rename, Refresh.
- You can only work with one form at a time: Therefore, the form list is not displayed in the main window.
- Forms are not saved in the database: They can only be saved as XML files.
- Versioning is not available when you save forms.
- Localization updates are limited. All changes made with the Caption Editor tool and all language updates installed on the server are unavailable. The Standalone Form Designer is delivered with its own language resource files (at the time of publishing, the available languages are English (US and UK), Canadian French, and Spanish).
- Changing captions of Yes/No questions and Five Rank Lists is not available.

Manually Installing the Form Designer (Standalone)

This application requires the mandatory resources contained in Desktop Resources. Ensure "Desktop Resources" on page 51 is installed on the desktop before proceeding.

1 Ensure all site preparation and system requirements are met for this application.

2 To start the installation wizard:

    - Double-click the **FormDesignerStandAloneInstallation.msi** icon.

- For **Windows Vista:** When the following message appears: **An unidentified program wants access to your computer**, click **Allow** to continue.

The **Welcome** screen of the Form Designer Standalone Setup wizard is displayed.

3 In the **Welcome** screen, click **Next**.

The End User License Agreement is displayed.

4 In the End User License Agreement screen, select **I accept the terms in the License Agreement**, and click **Next**.

The **Destination Folder** screen appears.

5 Select a destination folder for the Form Designer and click **Next.**

The recommended folder is **C:\Program Files\<Company Name>**.

6 Click **Next** to confirm the destination.

The **Ready to install** screen appears.

7 Click **Install** to begin the installation.

The installation starts. The status is displayed as the installation proceeds. The Completed Setup Wizard screen appears at the end of the setup.

8 Click **Finish** to exit the Setup Wizard.

9 To run the Form Designer, do one of the following:

- On the desktop, double-click the **Form Designer Standalone** icon.
- From the **Start** menu, go to **Programs > <Company Name>** and select **Form Designer Standalone**.

The **Standalone Form Designer** opens.

Uninstalling the Standalone Form Designer

1 From **Start >Settings > Control Panel**, open **Add or Remove Programs**.

2 Select the **Form Designer Standalone** option.

3 Click **Remove**.

The **Form Designer** is uninstalled.

Logger

Logger Overview

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.

For all software and hardware specifications refer to Chapter 2 “Customer Requirements”.

Manually Installing Logger

The manual installation procedure must be performed on the desktop on which the application will be run.

This application requires the mandatory resources contained in Desktop Resources. Ensure “Desktop Resources” on page 51 is installed on the desktop before proceeding.

To install Logger:

1. Download the installation package, according to “Downloading the Installation Packages” on page 24.
2. Run the **LoggerInstallation.msi** file.

   The **Welcome** screen of the setup wizard appears.
3. Click **Next**.

   The **End-User License Agreement** screen appears.
4. Select **I accept the terms in the License Agreement** and click **Next**.

   The **Custom Setup** screen appears.

   To view the required space for an application, select it in the list and read the text in the pane on the right.
5. Click **Next**.
6. 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** window appears.
7. Click **Install**.

   When the installation is complete, the **Installation Success** window appears.
8. Click **Finish** to exit the installation wizard.

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

9 Restart your computer.

Logger Silent Install Parameters

Refer to Chapter 3 “Installation by Role: Silent Distribution” for a sample script that includes the command line for distributing this application in silent mode.

The following 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

Phonetics Boosting

Phonetics Boosting Overview

Phonetics Boosting enables you to add new terms and phrases to the Speech Recognition engine's pre-defined vocabulary. It enables you to boost the recognition of all terms and phrases that are part of your company's vocabulary. Once a term is boosted, it will be better recognized and therefore be more effective in searches, categories and trends.

This chapter contains the information required to install Phonetics Boosting. For further information refer to the following documents:

- *Phonetics Boosting User Guide*

For all software and hardware specifications refer to Chapter 2 "Customer Requirements". The desktop must have at least 500 MB of free RAM space.

Manually Installing Phonetics Boosting

The Phonetics Boosting installation procedure must be performed on the desktop on which the Phonetics Boosting application will be run.

This application requires the mandatory resources contained in Desktop Resources. Ensure "Desktop Resources" on page 51 is installed on the desktop before proceeding.

To install Phonetics Boosting:

1. Double-click the **Phonetic Boosting Application Installer.msi** to launch the following Phonetics Boosting Application Setup Wizard:

2. Click **Next**.

   The window that appears includes the Phonetics Boosting End-User License Agreement.

3. Read the **End-User License Agreement**.

4. Select **I accept the terms in the License Agreement** and click **Next**.

   The **Custom Setup** window appears.

5. Click **Next**.

   The **Ready to install Phonetics Boosting Application** window appears.

6. Click **Install**.

   The **Installing Phonetics Boosting Application** window appears.

7 Click **Next**, once the Setup Wizard completes the Phonetics Boosting installation.

The **Completed the Phonetics Boosting Application Setup Wizard** window appears.

8 Click **Finish**.

Phonetics Boosting has been installed successfully.

Playback

Playback Overview

The **Playback** application is required on the workstations of users privileged to access audio and screen files from the Portal applications. Playback enables users to hear audio and see recorded screen activity, change the volume or speed of a call, jump to different points in a call, and see the waveform for an interaction.

The **Multimedia Support Package** incorporates codecs and infrastructure for the Playback controls. The package is installed automatically when installing Playback.

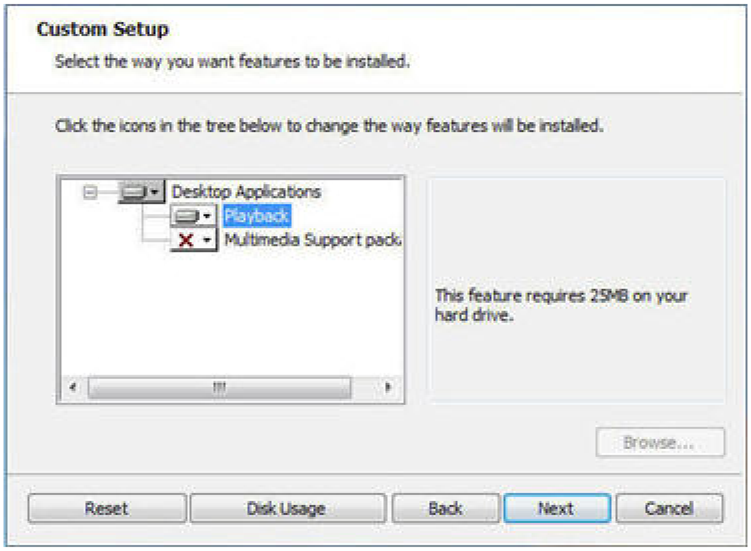
For all software and hardware specifications refer to Chapter 2 “Customer Requirements”.

Manually Installing Playback

Ensure all site preparation and system requirements are met before proceeding with the following installation instructions. This application requires the mandatory resources contained in Desktop Resources. Ensure “Desktop Resources” on page 51 is installed before proceeding.

1. Download the installation package, according to “Downloading the Installation Packages” on page 24.
2. Run the **PlaybackInstallation.msi** file. The **Welcome to the Playback Setup Wizard** screen appears.
3. Click **Next**. The **End-User License Agreement** screen appears.

4 Select **I accept the terms in the License Agreement** and click **Next**. The **Custom Setup** screen appears.



Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

This feature requires 25MB on your hard drive.

5 Select the relevant features to install:

- **To Install Playback** keep the default feature settings as they appear in the above image. It is not required to make the Multimedia Support Package available for installation as the Playback application incorporates this package and installs it automatically.
- **To Install the MultiMedia Support Package only:**

  Relevant when downloading audio files for playback on machines outside the enterprise or on machines 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:

Option	Description
Browse	Use to change the default destination folder. The Browse button is enabled when **Desktop Applications** is selected.
Reset	Click the Reset button to revert to the default installation settings.
Disk Usage	Click the Disk Usage button to view the disk space required compared to the disk space on the destination drives.

7 Click **Next**. The installer indicates if prerequisite software is missing. If required, stop the installation, install the prerequisite software are resume the installation. The **Playback Settings** screen appears.

8 If your system's audio and screen files are *not encrypted* click **Next.**

If your system's audio and screen files *are encrypted,* select **Encrypted Playback** and in the **Data Center Address** field, set the address of the server on which Data Center resides.

If your system's audio and screen files are encrypted, select **Encrypted Playback** and in the **Data Access Services Address** field, and enter the following address:

http: or https://<name of Application Server or Load Balancer>/KeyProxy/ManagementService.asmx

9 Click **Next**. The **Ready to Install** window appears.

10 Click **Install**. When the installation is complete, the **Installation Success** window appears.

11 Click **Finish** to exit the installation wizard. The **Installer Information** message appears prompting you to restart the computer.

12 Restart your computer.

NOTE 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 Playback

Refer to Chapter 3 "Installation by Role: Silent Distribution" for a sample script that includes the command line for distributing this application in silent mode.

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

Parameters	Description and Default Values
MsiFIle	PlaybackInstallation.msi
USE_COMMAND_LINE	USE_COMMAND_LINE=1 **Mandatory**
INSTALLFOLDER	Specifies the installation destination
PLAYBACK_ENCRYPTED	0 = Disable encrypted playback 1 = Enable encrypted playback **Default** = **0**
PLAYBACK_ENCRYPTIONWEBSERVICE	The address of the server on which Data Center resides. **Default=Empty**

Parameters	Description and Default Values
ADDLOCAL	Playback MultimediaSupportPackage **Default = Playback**
NOREBOOT	0 = Reboot 1 = No reboot **Default = 0**

Playback without Portal

When playback of audio files recorded by the system is required by users that do not have access to the Portal, including users outside the enterprise, the following methods can be used to playback the audio files:

TIP

Decrypted files only should be sent outside the enterprise, as playback of encrypted files require login to the Portal.

- **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. This method is supported from Windows XP Operating Systems and higher.
- **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.

SEE ALSO

For detailed information on the Media Encoder, see Appendix B “Media Encoder”.

Enabling Real Time Playback of Encrypted Screen Content in Transit

To enable real time playback of encrypted screen content in transit from the supervisor desktop, obtain the **client.wss** file and save it in the supervisor desktop in the installation folder (default: C:\Program Files\<Company Name>).

For details about obtaining the client.wss file, see the *Security Configuration Guide*.

Configuring Playback Stereo Recorded Contacts as Mono

You can configure the system to playback of stereo recorded contacts as mono recorded contacts.

The configuration is done by adding a new key to the registry.

Enabling Stereo Playback as Mono

1 Open **Notepad**.

2 Depending on the operation system, copy one of the following content into Notepad:

- For 32-bit operating system:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai]
"MonoToStereo"=dword:00000001
```

- For 64-bit operating system:

```
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 4, and double-click it.

A confirmation message appears.

5 Click **Yes**.

Disabling Stereo Playback as Mono

Disabling the stereo playback as mono functionality can be done by either updating the value of the **MonoToStereo** key in the registry or by deleting the key entirely.

To update the key:

1. Open **Notepad**.
2. Depending on the operation system, copy one of the following content into Notepad:
   - For 32-bit operating system:

     ```
     Windows Registry Editor Version 5.00

     [HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai]
     "MonoToStereo"=dword:00000000
     ```
   - For 64-bit operating system:

     ```
     Windows Registry Editor Version 5.00

     [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai]
     "MonoToStereo"=dword:00000000
     ```
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**.

To delete the key:

1. Go to **Start>Run** and type **Regedit**.
2. Depending on the operation system, locate one of the following registries:
   - For 32-bit operating system:

     ```
     [HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai]
     ```
   - For 64-bit operating system:

     ```
     [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\Samurai]
     ```
3. Right-click the **MonoToStereo** key and select **Delete**.

Pop-up Notification System

Pop-up Notification System Overview

The Pop-up Notification System, by default, is not privileged by any predefined user roles. When licensed, it is recommended to install the client on all workstations at the site.

The Pop-up Notification System client allows a WFO administrator, manager, supervisor, or scheduler to send pop-up messages to employees by selecting the recipients' name, login or role within the organization. Alternatively, administrators can configure automatic messaging based on conditions such as out of range KPIs or adherence issues. Three message templates are available to reflect high or normal priority, or confidentiality.

For all software and hardware specifications refer to Chapter 2 “Customer Requirements”.

Installing Pop-up Notification System Manually

The installation procedure must be performed on the desktop on which the application will be run.

To install Pop-up Notification System:

1. From the media, run the **PopupClient.msi** file.

   The **Welcome** screen of the setup wizard appears.

2. Click **Next**.

   The **License Agreement** screen appears.

3. Select **I accept the terms in the license agreement** and click **Next**.

   The **Destination Folder** screen appears.

4. Click **Next** to accept the default location, or click **Change** to define a different location, and then click **Next**.

   The **Server Configuration** screen appears.

5. In the **Domain Name** field, type the Domain name of the DNS that resolves the Pop-Up server. For example, **qa.bluepumpkin.local**.

6. (Optional) To configure the SSO Multiple domain mode, select **Do you wish to configure SSO Multiple Domain mode?** and then click **Next**.

   The **Ready to Install** window appears.

7. Click **Install**.

When the installation is complete, the **Installation Success** window appears.

8 Click **Finish** to exit the installation wizard.

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

9 Restart your computer.

NOTE If the pop-up client cannot be installed on port 2701, contact your business consultant regarding changing the Pop-up client command line options in order to change the port.

Pop-Up Notification Silent Install Parameters

The following properties determine how Pop-Up Notification is configured silently. Refer to Chapter 3 “Installation by Role: Silent Distribution” for a sample script that includes the command line for distributing this application in silent mode.

Parameters	**Description and Default Value**
MsiFile	PopupClient.msi
WS_SERVER	Domain name of the DNS that resolves the Pop-Up server. **Mandatory**.
INSTALLDIR	Specifies the installation destination Default = C:\<Company Name>\Pop-up Client
WS_MULTIDOMAIN	Specifies whether to configure the SSO Multiple domain mode. **Mandatory**. Valid values: Yes, No

Real Time Speech Calibration Application

Calibration Application Overview

The calibration application is used to enhance the accuracy with which keywords defined in Real Time Speech Notification rules are identified. The rules must be configured to trigger a calibration action in order for the recording to be marked as one to be examined with the calibration application.

The Analyst user examines the system's current accuracy in detecting keywords, can add new term pronunciations, and calibrates the system with an updated scoring method for term detection success.

This chapter contains the information required to install the application. For further information on using the application, refer to the following documents:

- *Real Time Speech Calibration Application User Guide*

For all software and hardware specifications refer to Chapter 2 "Customer Requirements".

Manually Installing Real Time Speech Calibration Application

The manual installation procedure must be performed on the desktop on which the application will be run.

This application requires the mandatory resources contained in Desktop Resources. Ensure "Desktop Resources" on page 51 is installed on the desktop before proceeding.

To install Real Time Speech Calibration Application:

1 Run the **Real Time Speech Validation Application.msi** file.

The **Welcome to the Real Time Speech Validation Application Setup Wizard** screen appears.

TIP The installer recognizes when the Multimedia Support Package is not installed the installation is terminated.

2 Click **Next**.

The **License Agreement** screen appears.

3 Select **I accept the terms in the license agreement** and click **Next**.

The **Destination Folder** screen appears.

4 Configure the following parameters:

- **Install Real Time Speech Validation Application to:** The default value is C:\Program Files\Impact360\....
- **Name of the Application Server or Load Balancer**.
- **SSL Only:** Select for systems configured to use SSL for client/server communication.
- **WFO Port:** Enter the port of the Framework Applications server role. Ensure the port is for SSL or non-SSL communication, whichever is relevant. The ports are listed in the *Firewall Ports Configuration Guide*.

5 Click **Next** and then **Install**.

When the installation is complete, the **Installation Completed** window appears.

6 Click **Finish** to exit the installation wizard.

A shortcut to the application appears on the desktop and can be accessed from the Start Menu in the Impact360 folder.

Calibration Application Silent Install Parameters

The following properties determine how the Real Time Speech Calibration Application is configured silently. Refer to Chapter 3 “Installation by Role: Silent Distribution” for a sample script that includes the command line for distributing this application in silent mode.

Parameters	Description and Default Value
MsiFile	Real Time Speech Validation Application.msi
USE_COMMAND_LINE	USE_COMMAND_LINE=1 **Mandatory**
INSTALLROOT	Specifies the installation destination Optional **Default = C:\Program Files\<Company Name>**
GLOBAL_APP_SERVER_DNS	Name of server hosting the Framework Applications Server role or Load Balancer. **Mandatory**.

GLOBAL_USE_SSL	Yes = SSL systems
	No = non-SSL systems
	Default = No

WFO_PORT	The SSL or non-SSL port number of the Framework Applications server role (hosted on the Application Server or Load Balancer) **Mandatory**

Screen Capture and AIM

Screen Capture and AIM Overview

Screen Capture and AIM includes three main 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.

This chapter contains the information required to install Screen Capture and AIM. For further information on using AIM, refer to the following documents:

- *AIM Quick Reference Guide*
- *AIM Online Help*

For all software and hardware specifications refer to Chapter 2 “Customer Requirements”.

Manually Installing Screen Capture and AIM

You can use the instructions in this section to perform a manual installation on an **agent workstation, a Terminal Server, a Citrix server, or a Virtual Machine**. The installation screens 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 following procedure.

To install Screen Capture and AIM:

1. Run as administrator the **Screen_Capture_Module.msi** file.

   The **Welcome** screen of the setup wizard appears.
2. Click **Next**.
3. One of two screens appears depending on whether you are installing the Screen Capture Module on a Terminal Server/Citrix server or on an agent workstation PC:

- **Destination Folder** - If this screen appears, skip to Step 5. This screen appears after the Welcome screen when you are installing the Screen Capture Module on an agent workstation PC.
- **Terminal Services configuration** - If this screen appears, continue to Step 4. This screen appears when you are installing the Screen Capture Module on a Terminal Server or Citrix Server.

4 The **Terminal Services configuration** screen settings are needed only if you use Quality Monitoring v7.8 (SP1 or 2) or v7.7 servers in your environment. Configure this screen as follows:

- If all of the servers in your environment are v11 (or v7.8) Recorder servers, delete any existing entries in the field provided for the BDR Server Name and Port Number. Then click **Next** and proceed to step 5.
- If you use Quality Monitoring v7.8 or 7.7 servers in your environment:

  i.In the field provided for the BDR Server Name and Port Number for the Terminal Services Adapter, type the host name of your BDR server and the port number on which the Terminal Services Adapter listens for connections.

  Separate the host name and port with a colon. For example, BDRServer1:3022.

  Separate multiple entries with a comma. For example, BDRServer1:3022,BDRServer2:3022

  ii.Select **Named Terminal Services Terminal** if your thin-client terminals are assigned host names.

  iii.Select **Anonymous Terminal Services Terminal** if you identify thin client sessions using the Windows username of the user.

  iv.Click **Next** to proceed to step 5.

5 In the **Destination Folder** screen, accept the defaults or click **Change** to select different destination folders for the Screen Capture software and its log files. Then click **Next**.

6 (Optional) In the **Data Security** screen, select **Data Encryption** to:

- Authenticate the connection from the Screen Capture Module to the Screen Recorder. If the authentication fails, the connection is terminated.
- Encrypt the recorded screen content while it is on the agent workstation before sending it to the network. This applies to screen capture communication with the recorder, and screen real time streaming to the supervisor desktop.

Then click **Next**.

7 In the **Integration Services Options** screen do one of the following:

- If you are installing the Screen Capture Module to work with Quality Monitoring Servers v7.8 (SP1 or 2) or v7.7, you do not need to configure this screen. Clear the **Connect to Integration Services** option, and click **Next** to continue to step 8.
- If you are installing the Screen Capture Module on a Terminal Services/Citrix Server, or on a PC configured in Enterprise Manager as a dynamic workstation, to operate with V11 (or v7.8) Recorder servers, do the following:

i. Select **Connect to Integration Services**.

ii. Type the host name and port of the server that hosts the Integration Service server role used by the v11 (or v7.8) Recorder server in the **Connect Adapter URL <hostname:port>** field, and then click **Next**.

For example: ISserver1:29522. Separate multiple entries with a comma. For example, ISserver1:29522,ISserver2:29522.

IMPORTANT Refer to the *Firewall Ports Configuration* spreadsheet.

Port 29522 is the default port in v11. In an upgrade scenario when the Integration Service is still at version 7.8 level, use port 3081. Once the Integration Service is upgraded to version 11 change the port to 29522.

- If you are installing the Screen Capture Module on Terminal Server or Citrix server, and you use Unify Servers to support CTI integration with v11 or v7.8 Recorder servers, do the following:

  i. Select **Connect to Unify Servers.**

  ii. Type the host name and port of the server that hosts the Unify Service server role used by the v11 or v7.8 Recorder servers in the **Connect Adapter URL <hostname:port>** field and then click **Next**.

  For example: UnifyServer1:3090. Separate multiple entries with a comma. For example, UnifyServer1:3090,UnifyServer2:3090.

8 In the **Agent Initiated Monitoring** screen, 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.
  - 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 checkmarks from all three options on this screen, and click **Next**. Skip to Step 12.

9 The **Quality Monitoring AIM Options** screen settings are needed only if the Screen Capture Module must operate with Quality Monitoring V7.8 (SP1 or2) or V7.7 servers in your environment. Configure this screen as follows:

- If all of the servers in your environment are V11 (or V7.8) Recorder servers, clear the **Connect to Quality Monitoring Server** option, and click **Next**. Proceed to Step 11.

- If you use Quality Monitoring v7.8 or 7.7 servers in your environment, do the following:

  i. Select **Connect to Quality Monitoring Server**.

  ii. In the **Quality Monitoring Connect Adapter URL <hostname:port> field**, type the hostname and port for the BDR server (the server on which the Quality Monitoring Connect Adapter resides). For example, BDRServer1:3020.

  iii. Select **Use CTI with AIM** to log on to AIM through CTI. With this option, the agent does not have to complete a separate login to use AIM.

  iv. Select **Use Manual Login** to prompt the agent to enter a user name and password before allowing the agent to use AIM. (If you do not select this option, skip Step 10 and proceed to Step 11 after completing this step.)

  v. Select **Enable anonymous terminal login with screen only workspaces** to allow anonymous terminal login to a workspace without a telephone (available only if you are installing the Screen Capture Module on a Terminal Server or a Citrix server).

  vi. Click **Next**.

10 If you select **Use Manual Login** in the previous step, the **Quality Monitoring Manual Logon Configuration** screen appears. This screen enables you to determine what entries (if any) appear by default to the user in the Agent ID and Agent Extension fields of the AIM login screen.

Configure the agent’s manual login credentials as follows:

- In the **Agent ID** field, type a value for the Agent ID field on the AIM login screen.

  If you leave this field blank, the agent must manually type the Agent ID in the AIM login screen (the field is not automatically populated).

- In the **Lock ID?** option, select **Yes** to prevent the agent changing the Agent ID that appears in the AIM login screen.

  Select **No** to allow the agent to change the Agent ID that appears in the AIM login screen.

- In the **Agent Extension** field, type a value for the Agent Extension field on the AIM login screen.

  If you leave this field blank, the agent must manually type the Agent Extension in the AIM login screen (the field is not automatically populated).

- In the **Lock Extension**? option, select **Yes** to prevent the agent changing the Agent Extension that appears in the AIM login screen.

  Select **No** to allow the agent to change the Agent Extension in the AIM login screen.

Then click **Next**.

11 In the **AIM Annotation Setup** screen, do one of the following:

- If you do not want to enable annotation for AIM, clear the checkmark from the **Enable annotation for Agent Initiated Monitors** option and click **Next**. Skip to Step 12.

- Select **Enable annotation for Agent Initiated Monitors** to enable annotation for AIM, and configure settings as follows:
  - In each required **User Field**, type a value.

    Values must exactly match what is configured for the Custom Attributes in the Quality Monitoring (V7.8 or 7.7 QM Servers) System Administration tool or Enterprise Manager (V11 or 7.8 Recorder servers). You do not have to enter a value in all five User Field boxes.
  - 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.
  - 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.
  - Click **Next**.

12 Click **Install**.

Configuring 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 to operate with either Quality Monitoring (QM) or V11 Recorders in a Citrix environment.

NOTE If you have a Citrix XP environment that does not use Terminal Services, skip the instructions in this section.

Use the following 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.

1 Launch the Microsoft Registry Editor.

2 Navigate to the following key:

```
HKLM\SOFTWARE\Witness Systems\eQualityAgent\Capture\CurrentVersion\
AdditionalUserApps
```

3 Add a string value (REG_SZ) to the key for each published application. Ensure that you observe the following restrictions:

- Value Name: Use any name that you want.

- Value Data: The value must match the name of the published application executable. Do not include the executable's path. For example, "MyApplication.exe".

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. As part of this configuration, the administrator uses the Enterprise Manager application to create workstation groups. When configuring the workstation groups, the administrator can configure three settings that control the quality of screen recording:

- Recording Quality/Data Rate
- Reduced Color
- Screen Change Detection Interval

Once these settings are configured in Enterprise Manager, the Recorder server sends them to the Screen Capture Module, and these settings control the quality of screen recording. If these settings are not configured in Enterprise Manager, the registry settings of the Screen Capture Module control the quality of screen recording.

SEE ALSO

- For more information on creating and configuring workstation groups, see the *Recorder Configuration and Administration Guide*.
- For more information on the Screen Capture registry settings, limitations and known issues, see Appendix A "Working with the Screen Capture Module".

Screen Capture and AIM Silent Install Parameters

The following mandatory and configurable parameters are for silently installing Screen Capture and AIM:

- Screen Capture Basic Install Parameters, page 78
- AIM Silent Install Parameters, page 80
- Terminal Services Server Silent Install Parameters, page 83

Refer to Chapter 3 "Installation by Role: Silent Distribution" for a sample script that includes the command line for distributing this application in silent mode.

Screen Capture Basic Install Parameters

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

Basic Parameters	Description and Default Values
INSTALLDIR	Specifies the installation destination **Default =** <Program Files>\<Company Name>\Screen Capture Module
ENCRYPTION_DATAENCRYPT	Determines whether or not data encryption is selected. TRUE = data encryption is selected. FALSE = data encryption is not selected. **Default** = NULL (FALSE). NOTE: If selected, make sure that Data Encryption is enabled in the System Administration Root Settings.
ENCRYPTION_WSSPATH	Specifies the path for the agent.wss file. Must be a valid Windows path. **Default =** same path as INSTALLDIR
AGENT_MONITORING_ENABLED	Determines whether or not to 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" on page 13
COLOR_REDUCTION	Determines the ColorReduction value. **Default** = 1 for new installations. For upgrades installations of Screen Capture retain the existing ColorReduction value. Can be changed by System Administrators in registry at HKEY_LOCAL_MACHINE \ SOFTWARE \ Witness Systems \ eQuality Agent \ Capture \CurrentVersion
CONN_INTG_SVC	Determines if there is a connection to an integration service. TRUE = connect to Integration Services is selected. Required in agent free-seating environments FALSE = connect to Integration Services is not selected. **Default** = NULL (FALSE) INTG_SERVER is enabled when CONN_INTG_SVC = TRUE
INTG_SERVERS	Relevant in agent free-seating environments. When CONN_INTG_SVC = FALSE, set parameter to an empty string. When CONN_INTG_SVC = TRUE, enter string of comma deliminated <server name>:<port number> pairs.
WDLS	Enable/disables SDK logging

AIM Silent Install Parameters

The following 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	Indicates whether the site uses CTI for recording.
	CTI = Use CTI for recording.
	MANUAL = Do not use CTI for recording.
	Default = CTI

CONNECT_ADPTR_URL	The server name and port number on which the Quality Monitoring Connect Adapter listens for requests. Syntax: CONNECT_ADPTR_URL=”<servername>:<port>” NOTE: Use with Quality Monitoring 6.x and above. Required. Port range: 0 - 65535. **Default =** Witness:3020.
MONITOR_BLOCK	Determines if agents have the ability to block capture sessions they initiate. TRUE = agents enabled to block monitoring they initiate. FALSE = agents not able to block monitoring they initiate. **Default:** NULL (FALSE).
ENABLE_ANNOT	Determines if agents have the ability to annotate captured sessions. TRUE = agents can annotate sessions they initiate. FALSE = agents cannot annotate sessions they initiate. **Default** = NULL (FALSE).

AIM Parameters	Description and Default Values
PAUSEMONITORING	The silent install inserts the DWORD value 'HKLM\SOFTWARE\Witness Systems\AIM\PauseMonitoring' into the Registry. Determines if agents have the ability to pause and resume monitoring a call for security and confidential card information reasons. 1 = agents can pause and resume contact recording 0 = agents cannot pause and resume contact recording, and cannot view the Pause Monitoring and Resume Monitoring AIM menu options. Any valid Windows path. **Default**: <Program Files>\Witness Systems\Screen Capture Module\Logs
AGENT_LOGS	Specifies the drive and path used by AIM to store and write log files. Any valid Windows path. **Default**: <Program Files>\Witness Systems\Screen Capture Module\Logs

Manual AIM Parameters	Description and Default Values
AGENT_EXTENSION	Use to automatically populate agent extension when they log on to AIM. Number. **Default**: 1234
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.

Manual AIM Parameters	Description and Default Values
AGENT_ID	Use to automatically populate agent ID when an agent logs on to AIM. Number **Default**: 1234.
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.

AIM Annotation Parameters	Description and Default Values
You must map these annotation properties to attributes using the Enterprise Manager. Annotations are considered customized attributes. For details, see the *Enterprise Manager System Administration Guide*.	
ANNOT_USER	Determines the user fields available for annotation. These fields must also be configured in the database, and configured in Quality Monitoring. Syntax: ANNOT_USER<n>=”UserField<n>” (where <n> is an integer from 1 to 5) String **Default:** UserFieldn. You do not have to provide values for all five fields.
USERTIP	Determines the user tips available for annotation. Syntax: USERTIP<n>=”<value n>” (where n is an integer from 1 to 5) String **Default:** This is User Field n. You do not have to provide values for all five fields.

Terminal Services Server Silent Install Parameters

The parameters in this 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	Determines whether anonymous terminal logon with screen only workspaces should be enabled. 1 = TRUE 0 = FALSE Any value other than 1, including nothing (NULL), equals 0 (FALSE). Only available for Quality Monitoring 6.x and above. Default: 0 (FALSE).
WS_TERMINAL_SERVER_LIST	BDR Server Name and Port Number for the Terminal Services Adapter in the format: <ServerName:Port>. Only available for Quality Monitoring 6.x. Default: Witness:3022
WS_TERM_SERVER_AGENTID	Choose from either the Named Terminal Services Terminal or the Anonymous Terminal Services Terminal. 0 (Named Terminal Services Terminal -Thin client terminals have hostnames assigned to them) 1 (Anonymous Terminal Services Terminal - Thin client sessions is identified using the Windows username of the user) Default: 0 (Named Terminal Services Terminal)

Strategic Planner Client

Strategic Planner Overview

Strategic Planner is a desktop resource for strategic resource planning that you can install in an MSSQL environment. Strategic Planner allows you to plan long term for multi-skilled contact center and enterprise back-office environments, assess the operational and financial benefits, and impacts 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, and provide executives with the information they need to review and rapidly approve budgets and plans.

For all software and hardware specifications refer to Chapter 2 “Customer Requirements”.

Manually Installing Strategic Planner

1. From the media, run the **Setup.exe** file.

   The **Welcome** screen of the setup wizard appears.
2. Click **Next**.

   The **License Agreement** screen appears.
3. Click **Yes** to accept the terms in the license agreement.

   The **Choose Destination Location** screen appears.
4. Click **Next** to accept the default location, or click **Browse** to define a different location and then click **Next**.

   When the installation is complete, the **Installation Success** window appears.
5. Click **Finish** to exit the installation wizard.

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

Configuring the Strategic Planner License Key

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.

Strategic Planner Silent Install Parameters

The following properties determine how Strategic Planner is silently configured. Refer to Chapter 3 “Installation by Role: Silent Distribution” for a sample script that includes the command line for distributing this application in silent mode.

Parameters	Description and Default Values
MsiFIle	Setup.exe
/s	**Mandatory**. Indicates silent mode.
/f1<path\ResponseFile>	**Optional**. The Response file contains all the values required for a silent install. **Default path =** Specifies the installation destination **Default ResponseFile** = setup.iss To change the default installation directory: **1** Copy the default response file, setup.iss, to "C:\temp" **2** Edit the setup.iss file by changing the value of **szDir** to "D:\Program Files\<Company Name>\Strategic Planner 7.9": **3** Run the installation silently from the command line: - Setup.exe /s /f1”c:\temp\setup.iss”

User Import Support Package

User Import Support Package Overview

This package is used for importing individual users from a Windows domain into the Enterprise User Manager. Bulk imports are not supported using this tool.

For all software and hardware specifications refer to Chapter 2 “Customer Requirements”.

Manually Installing User Import Support Package

The manual installation procedure must be performed on the desktop on which the application will be run.

To install User Import Support Package:

1 Run the **UserImportPackageInstallation.msi** file.

The **Welcome** screen of the setup wizard appears.

2 Click **Next**.

The **End-User License Agreement** screen appears.

3 Select **I accept the terms in the License Agreement** and click **Next**.

The **Custom Setup** screen appears.

To view the required space for an application, select it in the list and read the text in the pane on the right.

4 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** window appears.

6 Click **Install**.

When the installation is complete, the **Installation Success** window appears.

7 Click **Finish** to exit the installation wizard.

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

8 Restart your computer.

User Import Support Package Silent Install Parameters

Refer to Chapter 3 “Installation by Role: Silent Distribution” for a sample script that includes the command line for distributing this application in silent mode.

The following properties determine how User Import Manager is configured silently.

Basic Parameters	Description and Default Values
MsiFIle	UserImportPackageInstallation.msi
USE_COMMAND_LINE	USE_COMMAND_LINE = 1. **Mandatory**
VERINTFOLDER	Specifies the installation destination
GLOBAL_APP_SERVER_DNS	Name of the Application Server or Load Balancer. **Default = Empty**
GLOBAL_USE_SSL	0 = Do not use SSL. 1 = Use SSL. **Default = 0**

Chapter 5

Upgrading Desktop Applications

This chapter outlines the procedures required to upgrade Desktop Applications. The procedures for each application are listed and grouped according to the following previous versions:

Upgrading V11.1 Workstations

The customer is responsible to upgrade the desktop applications before system servers upgrade.

Upgrading to V11.1 SP1 desktops includes installing V11.1 SP1 clients on top of existing clients, while ensuring all V11.1 system requirements are met. Uninstall of existing desktop applications is not required.

All desktop applications are cross-compatible with Data Center server service pack levels, with the following exceptions:

- Forecast and Scheduling clients need to be upgraded at the same time as the Data Center servers.
- For systems upgraded fromV11.0 SP1 with end-to-end encryption, playback clients need to be upgraded before (or at the same time as) the Data Center servers.
- Screen capture desktops are compatible with Site servers. Therefore, you do not need to update screen capture desktops.

To upgrade desktop applications:

1. Ensure all customer requirements are met for V11.1 desktop applications. See Chapter 2 “Customer Requirements”.
2. **Download the most up-to-date installation packages** from the Latest Hotfixes area of the Online for Customer’s site. See “Obtaining the Installation Packages” on page 12.
3. **Install V11.1 SP1 desktop applications**. Follow the “Desktop Applications Installation Workflow” on page 10.

Upgrading V7 Recording Workstations

The version 7.8 Screen Capture Module and AIM Desktop Application compatible with V7.x Recorders can be upgraded to the version 11.1 Screen Capture Module and AIM for compatibility with Version 11.1 recorders.

1. Make sure the agent workstations meet the system requirements for the new version of the Screen Capture Module and AIM. See Chapter 2 “Customer Requirements”.
2. Upgrade the application by installing the new version manually or silently. See “Manually Upgrading Screen Capture Module and AIM” on page 90 or “Silently Upgrading Screen Capture Module and AIM” on page 90.

For a list of the versions of the V7.x Quality Monitoring software and the V11 Recorder servers compatible with this version of the Screen Capture Module, refer to Appendix A “Working with the Screen Capture Module” for further information.

Manually Upgrading Screen Capture Module and AIM

It is not required to manually uninstall the 7.8 version before installing the new version. Simply install the new version and the previous version is automatically removed while, all registry settings configured in the previous version are preserved.

Note that no indication is given that the older version was detected and removed. This is by design. The new version also preserves the agent.wss key file used by the old version. If encryption is enabled on the old version, preserving the agent.wss key file ensures that encryption is also enabled on the new version.

- For manual installations, see "Screen Capture and AIM" on page 73.

Silently Upgrading Screen Capture Module and AIM

When performing a silent installation, all registry settings configured in the previous version are preserved, except for those that are specifically configured with new values in the silent installation.

- For silent installation Parameters, see "Screen Capture and AIM Silent Install Parameters" on page 78.

Upgrading WFM Suite Workstations

The Desktop Applications compatible with previous WFO servers and their upgrade procedures are listed in the following table:

WFO Desktop Application	Upgrade Procedure
Forecasting and Scheduler	If upgrading from release 4.5.x or 4.6.x it is required to install the Director Enterprise Client. See Uninstalling the 4.5.x / 4.6.x Director Enterprise Client, page 91. Reinstall by running the following script located on the media: **<Desktop Applications installation folder>\ForecastingAndScheduling\ReInstallForecastingandScheduling.cmd** All default settings are automatically retrieved from the previous version and applied in the new version.
Strategic Planner	Install the new version. See "Strategic Planner Client" on page 84. Installing the new version automatically retrieves all default settings from the previous version.
Pop-Up Notification Client	Reinstall by running the following script located on the media: **<Desktop Applications installation folder>\Pop-up Client\ReInstall.cmd** All default settings are automatically retrieved from the previous version and applied in the new version.

Uninstalling the 4.5.x / 4.6.x Director Enterprise Client

Forecasting and Scheduling client installer uses MSI (Microsoft Installer) technology. It is required to first uninstall all previous InstallShield versions of the Director Enterprise clients before installing the new MSI version of Forecasting and Scheduling.

1 Click **Start > Settings > Control Panel > Add/Remove Programs.**

2 Select **Blue Pumpkin Director Enterprise Client**, and then click **Change/ Remove.**

3 In the Welcome screen, select **Remove**, and then click **Next**.

4 At the Confirm message, click **OK**

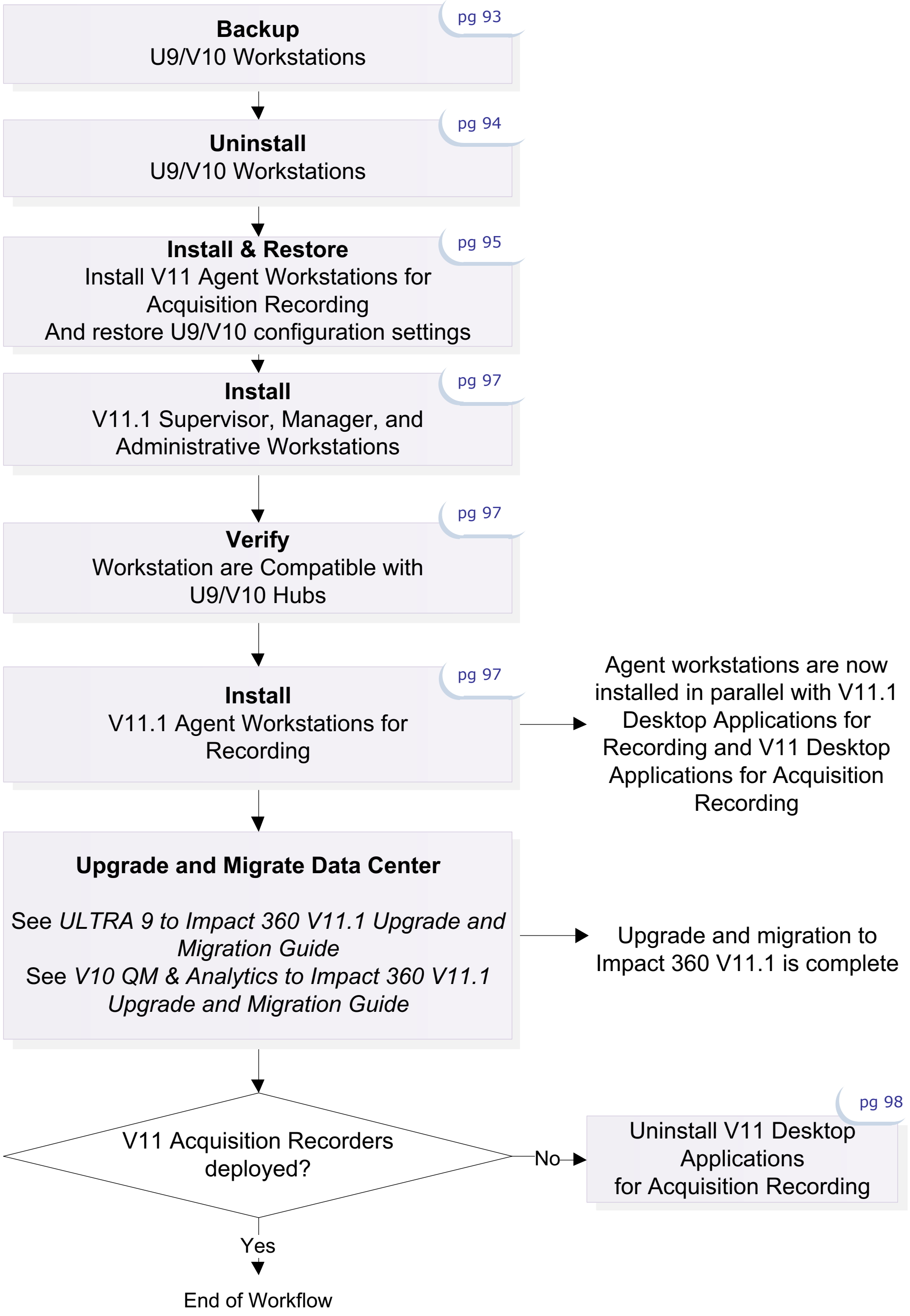
5 In the Maintenance Complete dialog box, click **Finish**.

Upgrading from ULTRA 9 or Impact 360 V10

Prior to upgrading and migrating the ULTRA 9 hubs or Version 10 data centers, all ULTRA 9 / V10 desktop applications must be upgraded. In addition, new V11.1 desktop applications are installed to support a transition to V11.1 recording or when expanding the solution with additional applications.

During the transition period before the data center is upgrades, V11.1 recording clients and V11.1 SP1 acquisition recording clients (including Citrix/terminal services environments) record side-by-side.

The below workflow must be followed when upgrading from ULTRA 9 or V10. On completing each procedure return to the workflow.


Backup
U9/V10 Workstations
pg 93
Uninstall
U9/V10 Workstations
pg 94
Install & Restore
Install V11 Agent Workstations for Acquisition Recording
And restore U9/V10 configuration settings
pg 95
Install
V11.1 Supervisor, Manager, and Administrative Workstations
pg 97
Verify
Workstation are Compatible with U9/V10 Hubs
pg 97
Install
V11.1 Agent Workstations for Recording
pg 97
Agent workstations are now installed in parallel with V11.1 Desktop Applications for Recording and V11 Desktop Applications for Acquisition Recording
Upgrade and Migrate Data Center
See *ULTRA 9 to Impact 360 V11.1 Upgrade and Migration Guide*
See *V10 QM & Analytics to Impact 360 V11.1 Upgrade and Migration Guide*
Upgrade and migration to Impact 360 V11.1 is complete
V11 Acquisition Recorders deployed?
No
Uninstall V11 Desktop Applications for Acquisition Recording
pg 98
Yes
End of Workflow

Backup ULTRA 9/V10 Workstations

Begin by backing up the registry keys. For backup it is required to export certain configuration registry keys to a backup location. This allows for the U9/V10 configuration settings to be later restored.

To back up U9/V10 registry keys:

1 Open the Registry Editor by selecting **Start>Run>Regedit.**

2 Right click the Registry Keys and select **Export.**

The relevant registry keys per application are listed here:

NOTE If a specific key does not exist, continue with the remaining keys and the procedure.

ULTRA V9 Desktop Applications	Registry Paths for Backup
Playback	[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Samurai\Proxy]
Record on Demand	[HKEY_USERS\.DEFAULT\Software\Comverse\RecordOnDemand] [HKEY_CURRENT_USER\Software\Comverse\RecordOnDemand] [HKEY_LOCAL_MACHINE\SOFTWARE\Comverse\RGC] [HKEY_LOCAL_MACHINE\SOFTWARE\Comverse\Apps]
Screen Acquisition Agent	[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Screens]
IntelliLink Agent	[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\ILA] [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ILA] [HKEY_LOCAL_MACHINE\SOFTWARE\Comverse\Install]

3 Save the relevant registration files (*.reg) at a backup location**.**

Uninstall ULTRA 9/V10 Workstations

After backing up the workstation registry keys, uninstall the ULTRA 9/ V10 desktop applications.

- Uninstalling ULTRA V9 Desktop Applications, page 94
- Uninstalling Impact 360 V10 Desktop Applications, page 95

Uninstalling ULTRA V9 Desktop Applications

Before you Begin

Before you uninstall the U9 Desktop Applications, set aside one workstation per site that is installed with the U9 Form Designer and U9 User Manager and do not uninstall this workstation. This is required for a gradual scenario. In addition, do not install Windows 7 on this machine.

Silent Uninstall

Use this method to uninstall all ULTRA V9 Desktop Applications simultaneously from multiple remote workstations using a batch file.

- Push the following command to the workstations:

  msiexec /x {982AF7AB-9939-11D6-817D-00105AB492EA}

  When this command is executed, all ULTRA V9 Desktop Applications on all the workstations are removed.

Manual Uninstall

Use this method to uninstall all the ULTRA V9 Desktop Applications on a workstation manually:

1 From **Add/Remove Programs:**

   a. Remove any **ULTRA U93 patches** from the workstations. For example:

   - ULTRA ILA patch U93_XXXX.
   - ULTRA Screen Agent patch U93SPX_XXXX
   - ULTRA Playback Patch U93_1866

   a. Select the **ULTRA 9 desktop** program and click **Remove**.

   All the ULTRA V9 Desktop Applications are removed from the workstation.

2 When prompted to restart the computer, click **Yes.** The computer reboots and the uninstall is complete.

Uninstalling Impact 360 V10 Desktop Applications

You can remove the entire Desktop installation, silently or manually:

- Silent Uninstall, page 95
- Manual Uninstall, page 95

Silent Uninstall

Use this procedure when you do not have access to the .msi file used to install Desktop applications.

1. From the **Start** menu, select **Run** to open the Command Line Interface (CLI).
2. Type **Cmd** and click **OK**.
3. Type

   ```
   msiexec /u {EB30A3F1-4CB4-45B0-833C-F186EF25484F}
   ```
4. Click **Enter** to remove all Desktop applications.
5. Restart your computer.

Manual Uninstall

1. From the **Start** menu, select **Settings > Control Panel > Add or Remove Programs** (Windows Vista, Windows 7 or Windows 2008) **or Programs and Features** (Other Windows platforms).
2. Select **Impact 360 Desktop Applications** and click **Remove**.

   The system removes all Desktop applications.
3. Restart your computer.

The computer reboots, and the uninstall process is complete.

Install and Restore V11 SP1 Agent Workstations for Acquisition Recording

After the ULTRA 9/V10 workstation backup and uninstall, install Agent Workstations with the most up-to-date V11 desktop applications for acquisition recording. The V11 acquisition clients are compatible with V11.1 systems.

1. Download the most up-to-date installation packages from the V11 SP1 Latest Hotfixes on the Verint Online for Customer’s site.

   a. Browse to **Impact 360 V11 > Support & Downloads > Latest Hotfixes and HFRs.**

   b. Expand the Hotfixes Tree to **Impact 360 V11 > V11.0 > SP1** and filter by **Desktop**.

   c. Click the Desktop Application from the **Subsystem** column and in the Subsystem Description window, click the **Download Link.** It is in the format KB106XXX.

d. In the Directory window, download the **KB11XXXX.zip** containing the up to date installation package for the desktop application.

2 Install agent workstations for acquisition recording. See Appendix C “Installing V11 SP1 Agent Workstations for Acquisition Recording”.

3 Restore the workstation configuration settings. See “Restoring Configuration Settings” on page 96.

Restoring Configuration Settings

Once the latest acquisition recording clients are installed, it is required to restore the configuration settings that were previously backed up.

1 Restore U9/V10 Registry Keys. This restores the Desktop Applications configuration settings.

a. Browse to the backup location of the registration keys defined in Step 3 of “To back up U9/V10 registry keys:” on page 93.

b. Double-click each registration file and then click **Yes** to add the information in the file to the registry.

2 For gradual upgrades, return **CTI Link Agent** Registry Key to ULTRA 9 Values.

During a gradual, site-by-site upgrade scenario, workstation support for ULTRA 9 is continued while workstation support for V11 is simultaneously introduced.

a. Browse to the registry: [**HKEY_LOCAL_MACHINE\SOFTWARE\Verint\ILA**]

b. Change to the value of the **ImpactVersion** key to **9**.

c. The CTI Link Agent interface appears with ULTRA V9 IntelliLink Agent terminology.

3 When the gradual upgrade to V11 Acquisition Recording is complete, update the registry keys to V11 values.

a. Review the registry keys of all installed Desktop Applications for the server or IP addresses and update them to the relevant V11 server address.

- For Agent Workstations with **V11 Screen Capture for Acquisition Recording**:

  Registry: [HKEY_LOCAL_MACHINE\SOFTWARE\Verint\ILA]

  Key: Infolink IP

  New Value: HTTP/HTTPS Alias of the server hosting the Acquisition Integration Service server role.

  Resolve the HTTP/HTTPS Alias by browsing to the Enterprise Settings and selecting the Consolidated or Acquisition Server > Additional Settings > HTTP/HTTPS Alias.

- For agent workstations with **V11 Record On-Demand**:

  Registry: [HKEY_LOCAL_MACHINE\SOFTWARE\Comverse\RGC]

  Key: ServerAddress

  New Value: HTTP/HTTPS Alias of the Application Server.

  Resolve the HTTP/HTTPS Alias alias by browsing to the Enterprise Settings and selecting the Consolidated or Application Server > Additional Settings > HTTP/HTTPS Alias.

b. For Agent Workstations with **V11 CTI Link Agent**:

   i. Browse to the registry: [**HKEY_LOCAL_MACHINE\SOFTWARE\Verint\ILA**]

   ii. Update the value of the **ImpactVersion** key to **11**.

c. The CTI Link Agent Interface is updated with V11 terminology.

Install V11.1 Supervisor/Manager and Administrator Workstations

1. Install V11 Supervisor/Manager Workstations
2. Install V11 Administrator Workstations
3. Install V11 Enterprise Administrate Workstations

   See Chapter 3 “Installation by Role: Silent Distribution” or Chapter 4 “Installation by Application”.

Verify V11 Workstation Compatibility with U9/V10 Hubs

At this stage, the Hubs are at U9/V10 level and the desktops are installed with V11 Desktop Applications. Perform the following sanity tests to verify acquisition compatibility.

1. From an Agent Workstation, use the Record On Demand (ROD) application to initiate recording.
2. From a Supervisor workstation, browse to the Portal and search for the contact recorded using ROD.
3. Verify that Playback of the recorded contact is working properly.

Install V11.1 Agent Workstations for Recording

This section is relevant for systems upgrading to V11.1 Recording. This in effect creates a side-by-side installation, whereby both V11 Acquisition Recording Desktop Applications and V11.1 Recorder Desktop Applications are installed on the same workstation. This is in preparation for transitioning to V11.1 Recording and allows you to work with U9/V10 and V11.1 in parallel.

- Install Agent Workstations with V11.1 Desktop Applications for Recording.

  See Chapter 3 “Installation by Role: Silent Distribution” or Chapter 4 “Installation by Application”.

Uninstall V11 Desktop Applications for Acquisition Recording

This section is relevant for systems that fulfill the following criteria:

- All sites and data center have fully transitioned to V11.1 Recording.
- No V11 Acquisition Recorders are deployed.

Uninstall	Manually	Silently
V11 Acquisition Screen Recording	From **Add/Remove Programs**, uninstall **Impact 360 ScreenRecording**	Run this script: **MsiExec.exe / I{F95B529F-C3F7-4212-AD59-A56F9C586151}**
V11 Record on Demand	From **Add/Remove Programs**, uninstall **Impact 360 Record On Demand**.	
V11 CTI Link Agent	From **Add/Remove Programs**, uninstall **Impact 360 ILA.**	Run this script: **MsiExec.exe /x {156688A2-30A0-46B6-A8D3-32E65C0951F2}**

Chapter 6

System Administration for Desktop Applications

Site-Dependent Playback (Optional)

Site-dependent playback means that the registry in the user's Desktop is configured manually to include a special key that indicates to the application's Locator to first search in all storage locations in a specific site for the contact before searching for the contact in other sites.

The purpose of site-dependent playback is to help minimize WAN traffic between different physical sites by prioritizing to stream a copy of the file that is *local*, rather than needlessly transferring data across the WAN.

This is an **optional configuration**. The system is developed to search for contacts to playback according to a default flow sequence. Configuring desktops with the Site ID overrides the default flow and is only relevant in cases of deployments with WAN connectivity.

Implementation involves configuring desktops with three registry keys with site ID for playback, telephony playback, and real-time monitoring.

- **Locator for site-dependent playback:** During playback, media is streamed to the desktop from the local site with a Content Server.
- **TPS for site-dependent telephony playback:** During telephony playback, playback lines are allocated to the desktop from the local site with a Telephony Playback Server or TPS Server Role to prevent long distance call tariffs.
- **RTP for site-dependent real-time monitoring:** During real-time monitoring, media is streamed to the desktop from the local site with an Integration Service server role mapped to the extension that is monitored.

SEE ALSO The *Technical Overview* details the default data flow for Playback, TPS and RTP. Site-dependent playback data flow is also detailed. See the chapter entitled Data Flows.

Configuring Desktops for Site-Dependent Playback

Complete this procedure following enterprise configuration.

1 In the Enterprise Settings, make a note of the Site IDs for the local Content Server, TPS and Recorder Integration Service.

The Enterprise Manager assigns a unique ID to each site or site group when the enterprise hierarchy is configured.

2 Update the following desktop registry key with site ID values for playback, telephony playback, and real-time playback.

For *Windows 32-bit systems*:

[HKEY_LOCAL_MACHINE\SOFTWARE\Verint\Desktop\SiteId]

For *Windows 64-bit systems*:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Verint\\Desktop\SiteId]

Set the following values (string, type REG_SZ):

- **Locator:** <ID of site with Content Server>
- **TPS:** <ID of site with Telephony Playback Service or TPS Service>
- **RTP:** <ID of site with Integration Service>

NOTE In regular TPS playback, Content Server selection is effected by the Site ID on the TPS and not by the Locator Site ID on the desktop.

Application Configuration Updates

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

- Server or Load Balancer Name Change, page 101
- Server Transition to/from SSL, page 101
- Transition to/from Encrypted Playback, page 102

Server or Load Balancer Name Change

There are Desktop Applications that rely on communication with the system server roles or Load Balancer (LB). When a change is made, a corresponding change to the Desktop Applications configuration is required.

Name changes can occur when:

- IT policy computer name changes
- Expansion scenarios
- Server joins a different domain
- Load Balancer (LB) name change

The configuration files to update are detailed according the relevant server role. See Updating Configurations by Server Role, page 102.

Server Transition to/from SSL

When moving the system to/from a secure SSL system and the server SSL certificate name was entered during the Desktop Applications installation, it is required to update the relevant configuration keys with the new certificate name.

The configuration files to update are detailed according the relevant server role. See Updating Configurations by Server Role, page 102.

Trusting SSL Certificate Authority

When an existing non-SSL system is transitioned to a SSL system, the desktop application initiates a handshake process with the server and the SSL server application responds with its own server certificate for verification. In order for Desktop Applications to trust the SSL server certificate, it must trust the Certificate Authority.

To this end, the certificate of the Certificate Authority must be included in the list of Trusted Root Certification Authorities stored on the workstations running desktop applications.

Transition to/from Encrypted Playback

Playback is configured for encryption during installation. If a change is made to or from encrypted playback, it is required to update the Playback configuration files.

The KeyProxyWebService playback registry key to update is detailed according the relevant server role. See Framework Applications/Interaction Applications Server Role, page 102.

In addition, it is required to reinstall Playback at SP1 level if an existing SP0 system with non-encrypted playback was upgraded to SP1. If there is no change to the encryption requirement, than reinstall of Playback is not required.

Updating Configurations by Server Role

This section details the configuration files that require updating, grouped by the server role that communicates with the desktop application.

- Recorder Integration Service Server Role, page 102
- Framework Applications/Interaction Applications Server Role, page 102

Recorder Integration Service Server Role

Screen Capture Module

Key: IntegrationServicesServersLis

Key Location: HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion

Update Required for SSL Transitions? Yes. For SSL support of Screen Transport Protocol see the section on Screen Encryption in the *Security Overview Configuration Guide*.

Framework Applications/Interaction Applications Server Role

- Playback, page 103
- Form Designer, page 103
- Real Time Speech Calibration Application, page 104
- Desktop Gadget, page 104
- Forecast and Scheduling, page 105
- Pop-up Notification Client, page 105

Playback

1 KeyProxyWebService

- Key Location:
  - On 32-bit versions of Windows: HKEY_LOCAL_MACHINE\SOFTWARE \<Company Name>\CryptoSDK
  - On 64-bit versions of Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\<Company Name>\CryptoSDK
- Key Value (string): https://<**server or LB name**>/KeyProxy/ManagementService.asmx
- Update required for SSL Transitions? Support for SSL is static. No change required.

2 AuthURL

- Key Location: HKEY_LOCAL_MACHINE\SOFTWARE\<Company Name>\CryptoSDK
- Key Value (string): http://<**server or LB name**>:<7001/wfo/control/signin
- Update required for SSL Transitions? **Yes.** When moving to SSL it is required to change HTTP to HTTPS, and to change the port number to 7002.

Form Designer

1 Verint.EvaluationPackage.FormManagement.FormManagementControlLibrary.FormManagementWS.FormManagementWS

- Key Location: <Software Drive>:\Program Files\<Company Name>\FormDesigner\Verint.EvaluationPackage.FormManagement.FormManagementUI.exe.config
- Key Value (string): http://<**server or LB name**>/FormManagementWS/FormManagementWs.asmx
- Update required for SSL Transitions? No change required.

2 Verint.EvaluationPackage.FormManagement.FormManagementControlLibrary.FormManagementWS.FormManagementWS.HTTPS

- Key Value (string): https://<**server or LB name**>/FormManagementWS/FormManagementWs.asmx
- Update required for SSL Transitions?: No change required.

3 FilloutPathForPreview

- Key Value (string): http://<**server or LB name**>/Fillout/EvaluationForm.aspx
- Update required for SSL Transitions?: **Yes**

4 AuthUrl

- Key Value (string): http://**<server or LB name:7001>**/wfo/control/signin?screen=QM_ACTIVEX_LANDING_PAGE&amp;integrationURL=magic
- Update required for SSL Transitions? **Yes**

Real Time Speech Calibration Application

1 Server

- Key Location: HKEY_LOCAL_MACHINE\SOFTWARE\Impact360\KWS Calibration
- Key Value (string): <**server or LB name**>
- Update required for SSL Transitions?:No

2 SSL

- Key Location: HKEY_LOCAL_MACHINE\SOFTWARE\Impact360\KWS Calibration
- Key Value: Yes/No
- Update required for SSL Transitions: **Yes**

3 WFO Port

- Key Location: HKEY_LOCAL_MACHINE\SOFTWARE\Impact360\KWS Calibration
- Key Value: <**WFO Port>**
- Update required for SSL Transitions: **Yes**

Desktop Gadget

1 Serverurl

- Key Location: HKEY_LOCAL_MACHINE\SOFWARE\Wow6432Node\Impact360\DesktopGadget
- Key Value: http://**<server or LB name:7001>**/wfo/
- Update required for SSL Transitions: **Yes**

2 SSOmode

- Key Location: HKEY_LOCAL_MACHINE\SOFWARE\Wow6432Node\Impact360\DesktopGadget
- Key Value: <**true**>
- Update required for SSL Transitions: No

3 Serverurl (user)

- Key Location: HKEY_CURRENT_USER\SOFWARE\Wow6432Node\Impact360\DesktopGadget
- Key Value: http://**<server or LB name:7001>**/wfo/
- Update required for SSL Transitions: **Yes**

4 SSOmode (user)

- Key Location: HKEY_CURRENT_USER\SOFWARE\Wow6432Node\Impact360\DesktopGadget
- Key Value: <**true**>
- Update required for SSL Transitions: No

Forecast and Scheduling

In this case, the Framework Application Server or Application Load Balancer name is updated from within the application manually:

1. In the login window, hold the **Ctrl+Shift** keys and click **User Name**.
2. Update the Application Server or Load Balancer name and port.

If SSL is enabled, no additional configuration is required as all web pages launched from the application automatically uses SSL. However, if the system is transitioned from SSL to non-SSL, Forecasting and Scheduling retains the SSL configuration. Please contact your account manager to revert to non-SSL.

Pop-up Notification Client

The Pop-up Notification systems works by SIP based client-server communication. DNS_SIP entries in the IP network containing the pop-up server's name and domain are located by the pop-up client as required.

Perform the steps in this section if you are changing the computer name and/or the domain membership of the pop-up server(s).

To update server name when workstation and server are in the same domain:

- Update the **DNS _SIP** entry to point to the correct server. This is a manual procedure and performed by the customer.

To update domain membership when workstation and server are in the same domain:

1. Create new **DNS _SIP** entry in the new domain. This is a manual procedure and performed by the customer.
2. Update all Pop-up clients with the new domain. This is performed by the customer, usually by SMS push to all workstations.
3. Update the Pop-up domain name in the Pop-up Server configuration:
   a. In the Enterprise Manager Server Settings, select the **Framework Applications Server Role**.
   b. In the **Pop-up Server** section, enter the new **Pop-up Domain** value and **save** the configuration. This distributes the domain membership change to the .inin and bpmaindb files.

To update domain membership of the workstations only:

- Update the **DNS _SIP** entry to point to the correct domain. This is a manual procedure and performed by the customer.

Appendix A

Working with the Screen Capture Module

You can install the Screen Capture Module to work with the Recorder server, the Quality Monitoring Application, or the Version 7 Quality Monitoring Product. For Screen Capture Module installations instructions, see "Screen Capture and AIM" on page 73.

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

This appendix discusses the following topics:

- Screen Capture Module Compatibility, page 107 - Lists the versions of the Quality Monitoring software and the Recorder servers that are compatible with this version of the Screen Capture Module.
- Installation in a Citrix or Terminal Services Environment, page 108 - 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 to understand how to get optimum performance from Screen Capture Modules installed in a Citrix or Terminal Services environment.
- Screen Capture and AIM Registry Settings, page 111 - Discusses all of the registry settings for the Screen Capture component and the Agent Initiated Monitoring (AIM)

component of the Screen Capture Module. Use the registry settings to fine tune the performance or to change the application configuration after it is installed.

- Configurations Needed to Support AIM Call Annotation, page 124 - Explains all configurations you must perform to enable agents to annotate calls from the AIM application.
- Enabling Multi-Monitor Screen Capture Support, page 129 - Explains how to record screen images on agent workstations that have multiple monitors.
- Known Issues, page 130 - Discusses the known issues with the Screen Capture Module.
- CapTestB Utility, page 135 - Typically installed on an IT Administrator workstation for testing the performance of the screen capture application installed on the Agent Workstation for Recording.

Screen Capture Module Compatibility

This table describes the Screen Capture Module 11.0 compatibility with different versions of the Quality Monitoring software and the Recorder server. Review this information when installing the Screen Capture Module in environments that include both V11 servers and servers from earlier releases.

NOTE In the V11 release, the Quality Monitoring Application (along with other applications) is available on a server that has the Interaction Applications server role activated. With the Version 7 Quality Monitoring releases, the QM software was deployed on a dedicated server.

The Screen Capture Module 11.0 can work with the Quality Monitoring software and Recorder versions listed in this table.

Supported Versions	Comments
Quality Monitoring	
11.0	Fully Supported
7.8 SP2	Fully Supported
7.8 SP1	Fully Supported
7.7	Partially Supported*
Recorder	
11.0	Fully Supported
7.8	Fully Supported

Quality Monitoring v7.8.2 product and Recorder v11 server compatibility with different versions of Screen Capture Module:

Screen Capture Module Version	QM 7.8.2	Recorder V11
11.0	Fully Supported	Fully Supported
7.8 SP2 QM	Fully Supported	Fully Supported
7.8 SP1	Fully Supported	Only Desktop Screen Capture is supported. Citrix and Terminal Services are not supported.
7.8 - Recorder	Fully Supported	Only Desktop Screen Capture is supported. Citrix and Terminal Services are not supported.
7.7 - QM	Partially Supported*	Not Supported.
7.6, 6.5, 6.4 and 6.3	Not Supported	Not Supported.

* Supported only if Data Encryption features are disabled (the data encryption algorithm changed from the Blowfish Algorithm to the AES256 algorithm). To disable Data Encryption, disable the Data Encryption setting during the Screen Capture installation, or set the DataEncryption registry setting to 0, as discussed in "Screen Capture Registry Values" on page 112.

Installation in a Citrix or Terminal Services Environment

This section discusses special considerations and configurations of which you should be aware when installing the Screen Capture Module on a Citrix or Terminal Services server. This section discusses the following topics:

- Supported Terminal Server Sessions, page 108
- Limitations and Best Practices, page 109
- Memory Utilization on a Terminal Server, page 111

Supported Terminal Server Sessions

For details about supported Citrix or Terminal Services environments, see "Thin Clients and VMware" on page 17.

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 server also supports Agent Initiated Monitoring (AIM) in remote sessions where the system tray is displayed; the AIM icon is available only in the system tray.

The 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.

VMware Environments and Screen Capture

The information in this section applies only to Screen Capture for Agent Workstations in Quality Monitoring (QM) environments.

If VMware Infrastructure (ESX) is used, a static host name is required per virtual machine. We recommend using Dynamic Workspaces with Agent Initiated Monitoring (AIM) in Virtual Desktop Infrastructure (VDI) environments. AIM is used to register a logon from the Virtual Desktop to the BDR when the agent logs in.

If it is not feasible to use Dynamic Workspaces, you can use Static Workspaces with the following requirements:

- A “fixed seating” environment must be in place with respect to the telephone. The agent must sit at the same fixed extension, or “carry” the extension with him/her in an environment that supports extension mobility.
- The VDI system should be configured for a persistent pool of virtual desktops.
- We recommend that the persistent pool of virtual machines be pre-assigned to the agents to allow the workspaces to be created in Quality Monitoring and assigned to the proper telephone. This can be accomplished in VMware View using the VMware View Manager tool.

Limitations and Best Practices

There are some limitations surrounding screen capture of multiple sessions and/or Published Applications in Windows Terminal Services and Citrix environments. This section discusses best practices you can employ to minimize these limitations.

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 will record all activities in that Desktop session.
- An individual Published Application session, then it will record 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 will 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” on page 110 for instructions on

configuring explorer.exe as the Published Application.

- A session that is shared between Published Applications, then it will record all the Published Applications in that session. Published Applications with common properties (color depth, resolution, encryption etc.) can be configured to share the same session within Citrix. Refer to http://support.citrix.com/kb/entry.jspa?externalID=CTX159159 for session sharing details.

The limitations for the capture are as follows:

- Multiple simultaneous sessions cannot be recorded, as noted below:
  - If the agent opens multiple Published Applications (not by session sharing) from a single Citrix Server, then recording of only one session will occur.
  - If the agent opens multiple Published Applications from different Citrix servers in a Citrix server farm, then recording of only one session will occur.
- The session that is recorded is the session most recently created. For example, if the agent first opens Email as a published application on one server and then CRM as an application on a different server, the CRM application session will be recorded and associated with his next call. If he opens CRM first and Email second, then Email will be recorded.

Configuration Details

To enable the recording of all Published Applications in circumstances where the determination of which screen should be recorded is not predictable:

- Restrict each agent to work on 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 to share the same 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 short cuts to applications. When the explorer.exe is launched on the client PC, it opens the folder containing the shortcuts. Only one session will be created on the Citrix Server when explorer.exe program is launched. Use the shortcuts available from the folder in explorer.exe to launch the applications. All applications launched using the shortcuts will run in the same explorer.exe session.

Windows Terminal Services (without Citrix) Screen Capture Limitations

In capturing screens under Windows Terminal Services, the Recorder records only one Windows Terminal Session at a time per agent. It records all the activities in that Terminal Session.

The limitations of the capture are as follows:

- If the agent opens Multiple Terminal Sessions from different Windows Terminal Servers then recording of only one session will occur.
- If the agent opens Multiple Terminal Sessions from a single Windows Terminal Server then recording of only one session will occur.
- The session that is recorded is the session most recently created. For example, if the agent first opens Email on one server and then CRM as an application on a different server, the CRM application session will be recorded and associated with his next call. If the agent opens CRM first and Email second, then Email will be recorded instead.

Configuration Details

To enable the recording of all activities in circumstances where the determination of which screen should be recorded is not predictable:

- Restrict each agent to working on a single Windows Terminal Server and to the single Terminal Session. Allow the agent to access all of the applications through the terminal session.

Memory Utilization on a Terminal Server

Use the following formula to estimate the capture memory utilization:

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

Screen Capture and AIM Registry Settings

You can change the Windows registry settings after installation to fine tune the Agent Capture Service or Agent Initiated Monitoring (AIM) performance or to enable additional capabilities in these applications after the applications have been installed.

This section provides reference information for all of the registry keys available for the Agent Capture Service and the Agent Initiated Monitoring (AIM) applications, including the possible values for each key.

Registry Key Locations

The Screen Capture registry keys are located in:

`HKLM\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion`

For information on the individual Agent Capture Service registry keys, see “Screen Capture Registry Values” on page 112 and “Registry Values for Terminal Services Support” on page 116.

The AIM registry keys are located in:

HKLM\SOFTWARE\Witness Systems\AIM

For information on the individual AIM registry keys, see “AIM Registry Values” on page 116.

WARNING Use caution when changing registry values. Editing the registry may cause the program to become unstable.

Screen Capture Registry Values

The Screen Capture registry keys are located in:

HKLM\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion

Screen Capture uses the following registry values. The Screen Capture executable name is WcapW32.exe.Setting Specific Agent Capture Service Entries

Registry Entry	Description	Type	Default Value
CaptureMethod	Screen capture method: 1 - Enhanced 2 - Normal	REG_DWORD	1
DualMonitor	Add this setting if it is missing in the registry. Values include: 0 - Dual monitor recording disabled 1 - Dual monitor recording enabled See “Configurations Needed to Support AIM Call Annotation” on page 124 for specific details on the dual monitoring recording support.	REG_DWORD	1
CaptureRunPath	Agent Capture Installed directory path.	REG_SZ	“”
CompressionMethod	Compression algorithm to use: 1 - Enhanced 2 - Normal 3 - Microsoft RLE8 4 - JPEG Compression 5 - 5.x Compatible 6 - 6.x Compatible (6.3 and below)	REG_DWORD	1
ColorReduction	Reduce the number of colors captured to 256. 0 - Off 1 - On	REG_DWORD	0

Registry Entry	Description	Type	Default Value
AgentSocketPort	Socket TCP port number to listen on for connection request from the recorder server when the Screen Capture Module is installed on an agent's PC.	REG_DWORD	4001
EnhancedResolution	Causes Capture to continuously fake a constant monitor to artificially use CPU and memory resources even when a monitor is not in progress: 0 - Off 1- On	REG_DWORD	0
WSSPath	Directory path to the "agent.wss" file used by WCapW32.exe during server authentication and data encryption.	REG_SZ	""
DataEncryption	If this is set to 1, Capture encrypts the screen data before sending it to the recorder server. 0 - Not Encrypted 1 - Encrypted	REG_DWORD	0
ScreenChangeDetectionInterval	This setting defines how often (in msec) the capture will check for screen changes. The setting range is 25 - 500. Lowering the value will increase the capture quality and the amount of CPU used by capture. The setting can be automatically adjusted by the capture if the CPU utilization exceeds the value set by the MaxAvgCPU.	REG_DWORD	150
CaptureLayeredWindows	Set this value to 1 to captured layered windows, such as transparent windows, tool tips, etc. Setting this value to 1 increases the Screen Capture software CPU utilization. 0 - Enabled 1 - Disabled	REG_DWORD	0
CompressionQuality	Compression Quality in the range 1 to 10 10 - Best compression (Low Performance) 1 - Less Compression (Best Performance) **Note:** This setting applicable only when 'CompressionMethod' is 1 or 4.	REG_DWORD	5
MaxAvgCPU	The setting limits the amount of CPU (in percents) the capture can use.	REG_DWORD	60

Registry Entry	Description	Type	Default Value
IntegrationServicesServerList	Comma-separated list of the Integration Services server names to be serviced by the Capture Service.	REG_SZ	""
UnifyServersList	Comma-separated list of the Unify server names to be serviced by the Capture Service in a Terminal Services environment.	REG_SZ	""
CaptureQuality	Can be changed from 1 to 10, where 10 indicates the highest quality. Increasing the setting results in higher CPU utilization.	REG_DWORD	7

Setting Specific Screen Capture Entries

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

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

IMPORTANT The registry settings discussed below all affect the image quality of screen captures. You can also specify similar settings that affect the image quality of screen captures from the Enterprise Manager application when configuring workstation groups for screen recording.

If an image quality setting is specified for a workstation group in Enterprise Manager, that setting takes precedence over the registry setting. For more information, see "Screen Capture and AIM Post Installation Notes" on page 78.

CaptureMethod

Set the CaptureMethod to 1 (Enhanced) for a good screen change detection method. When CaptureMethod is set to 1, the screen recording playback usually has no tiling behavior; however, the playback uses more CPU than other methods.

Set the CaptureMethod to 2 (Normal) for efficient CPU utilization. When CaptureMethod is set to 2, you may see tiling in the playback.

CompressionMethod

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

Compression Method	Avg. Compression Ratio
Normal Compression	8:1
Microsoft RLE8 Compression	2:1
Enhanced Compression	40:1
JPEG Compression	40:1

NOTE

1. The compression ratio may vary depending on the screen bitmaps being compressed.
2. Compression methods providing better compression ratio usually use more CPU.
3. JPEG compression provides the best compression when capturing pictures, but it may cause loss of quality in the images when the recording is played back.

CompressionQuality

The Compression Quality entry is applicable only when 'Enhanced Compression' or 'JPEG 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 will have the ColorReduction value set to `1` (on). However, upgrade installations of the Screen Capture Module will keep the existing ColorReduction value.

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

The advantage of color reduction is that it results in small packets and uses less network bandwidth and less disk space to store the screen capture files.

Color reduction is more suitable when the agents are using Notepad, Word and Outlook kind of applications, since these applications produce less color data.

ScreenChangeDetectionInterval

The ScreenChangeDetectionInterval defines how often (in msec) the capture will check 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.

Registry Values for Terminal Services Support

The registry values for Terminal Services Screen Capture support are located in:

`HKLM\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion`

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
WitnessServerList	Comma-separated list of the QM BDR server names to be serviced by the Capture Service on the Terminal Services servers.	REG_SZ	Blank
TermSvr	Used to indicate thin-client server: 0 - Not Terminal Server 1 - Terminal Server	REG_DWORD	1
UseAgentID	Used by the Capture Service for Terminal Services servers to determine whether device host names or agent logon IDs are used to locate thin-client sessions: 0 - Device Host Name 1 - Agent Logon ID	REG_DWORD	0
ServiceSocketListenPort	Capture service socket port for listening for recorder server connections in Terminal Services environments. Typically 4002.	REG_DWORD	4002

AIM Registry Values

The AIM registry keys are located in:

`HKLM\SOFTWARE\Witness Systems\AIM`

Agent Initiated Monitoring uses the following registry values.

Registry Entry	Description	Type	Default Value
EnableAnnotation	Enables the Annotate option in the AIMTray menu.	REG_DWORD	1
Client_AdapterURL	**Applicable only in QM environments.** QM BDRServer name and port number separated by a colon (:) to which AIM event messages are sent. Clear this setting value for Recorder server environments.	REG_SZ	\`\`\`\`

<table>
<tr><th>Registry Entry</th><th>Description</th><th>Type</th><th>Default Value</th></tr>
<tr><td>Client_Trace</td><td><b>Applicable only in QM environments.</b>
Used for debug purposes only. When this setting is enabled, AIM displays the event message that is being sent to BDR Server in the message box
1 - Enable
0 - Disable</td><td>REG_DWORD</td><td>0</td></tr>
<tr><td>LockAgentID</td><td><b>Applicable only in QM environments.</b>
When this setting is set to 1, AIM disables the Agent ID field from editing in the AIM Login dialog box.
1 - Disable
0 - Enable</td><td>REG_DWORD</td><td>0</td></tr>
<tr><td>LockExtension</td><td><b>Applicable only in QM environments.</b>
When this setting is set to 1, AIM disables the Agent Extension field from editing in the AIM Login dialog box.
1 - Disable
0 - Enable</td><td>REG_DWORD</td><td>0</td></tr>
<tr><td>LogonLogoff</td><td><b>Applicable only in QM environments.</b>
Set to 1 to display the Logon/Logoff Agent options in AIMTray menu.
1 - Display
0 - Hide</td><td>REG_DWORD</td><td>0</td></tr>
<tr><td>StartMonitoring</td><td>Set this value to 1 to display the Start Monitoring option in AIMTray menu.
1 - Display
0 - Hide</td><td>REG_DWORD</td><td>1</td></tr>
<tr><td>StartStopBehavior</td><td>Specifies events that are sent for Start Monitoring and Stop Monitoring commands:
<table>
<tr><th>Value</th><th>Start Monitoring events</th><th>Stop Monitoring events</th></tr>
<tr><td>0</td><td>StartRecord</td><td>StopRecord</td></tr>
<tr><td>1</td><td>Connected</td><td>Disconnected</td></tr>
<tr><td>2</td><td>Connected, StartRecord</td><td>StopRecord, Disconnected</td></tr>
</table></td><td>REG_DWORD</td><td>0</td></tr>
</table>

Registry Entry	Description	Type	Default Value
StartStopContentType	Specifies media type for Start and Stop Monitoring commands: AudioVideo - audio and screens Audio - audio only Video - screens only	REG_SZ	AudioVideo
StopMonitoring	Set this value to 1 to display the Stop Monitoring option in AIMTray menu. 1 - Display 0 - Hide	REG_DWORD	1
Client_UseStub	**Applicable only in QM environments.** Used for Debug purpose only. AIM drops the messages when it is set to 1 (messages will not reach BDR Server).	REG_DWORD	0
Client_ReturnFailure	**Applicable only in QM environments.** Used for debug purposes only. When set to 1 it tracks the success or failure of the messages sent to the BDR Server. 1 - Enable 0 - Disable	REG_DWORD	1
Client_AutoReconnect	**Applicable only in QM environments.** Used for Debug purposes only. Configures AIM to auto reconnect if the connection to the BDR Server is broken. 1 - Reconnect 0 - Do not reconnect	REG_DWORD	1
BlockMonitoring	Set this value to 1 to display the Block Monitoring option in the AIMTray menu. 1 - Display 0 - Hide	REG_DWORD	1
UserFieldName1	Specifies the User Field 1 custom attribute name.	REG_SZ	Contact.AIM.User1
UserFieldName2	Specifies the User Field 2 custom attribute name.	REG_SZ	Contact.AIM.User2
UserFieldName3	Specifies the User Field 3 custom attribute name.	REG_SZ	Contact.AIM.User3
UserFieldName4	Specifies the User Field 4 custom attribute name.	REG_SZ	Contact.AIM.User4

Registry Entry	Description	Type	Default Value
UserFieldName5	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
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
StartMonitoringAnnotationFieldName1	Specifies the field name that is tagged in Start Monitoring command.	REG_SZ	“”
StartMonitoringAnnotationFieldName2		REG_SZ	“”
StartMonitoringAnnotationFieldName3		REG_SZ	“”
StartMonitoringAnnotationFieldName4		REG_SZ	“”
StartMonitoringAnnotationFieldName5		REG_SZ	“”

Registry Entry	Description	Type	Default Value
StopMonitoringAnnotationFieldName1	Specifies the field name that is tagged in Stop Monitoring command.	REG_SZ	
StopMonitoringAnnotationFieldName2		REG_SZ	
StopMonitoringAnnotationFieldName3		REG_SZ	
StopMonitoringAnnotationFieldName4		REG_SZ	
StopMonitoringAnnotationFieldName5		REG_SZ	
BlockRecordingAnnotationFieldName1	Specifies the field name that is tagged in Block Recording command.	REG_SZ	
BlockRecordingAnnotationFieldName2		REG_SZ	
BlockRecordingAnnotationFieldName3		REG_SZ	
BlockRecordingAnnotationFieldName4		REG_SZ	
BlockRecordingAnnotationFieldName5		REG_SZ	
PauseRecordingAnnotationFieldName1	Specifies the field name that is tagged in Pause Recording command.	REG_SZ	
PauseRecordingAnnotationFieldName2		REG_SZ	
PauseRecordingAnnotationFieldName3		REG_SZ	
PauseRecordingAnnotationFieldName4		REG_SZ	
PauseRecordingAnnotationFieldName5		REG_SZ	

Registry Entry	Description	Type	Default Value
ResumeRecordingAnnotationFieldName1	Specifies the field name that is tagged in Resume Recording command.	REG_SZ	
ResumeRecordingAnnotationFieldName2		REG_SZ	
ResumeRecordingAnnotationFieldName3		REG_SZ	
ResumeRecordingAnnotationFieldName4		REG_SZ	
ResumeRecordingAnnotationFieldName5		REG_SZ	
StartMonitoringAnnotationFieldValue1	Specifies the field value that is tagged in Start Monitoring command.	REG_SZ	“”
StopMonitoringAnnotationFieldValue2		REG_SZ	“”
StartMonitoringAnnotationFieldValue3		REG_SZ	“”
StartMonitoringAnnotationFieldValue4		REG_SZ	“”
StartMonitoringAnnotationFieldValue5		REG_SZ	“”
StopMonitoringAnnotationFieldValue1	Specifies the field value that is tagged in Stop Monitoring command.	REG_SZ	
StopMonitoringAnnotationFieldValue2		REG_SZ	
StopMonitoringAnnotationFieldValue3		REG_SZ	
StopMonitoringAnnotationFieldValue4		REG_SZ	
StopMonitoringAnnotationFieldValue5		REG_SZ	

Registry Entry	Description	Type	Default Value
BlockRecordingAnnotationFieldValue1	Specifies the field value that is tagged in Block Recording command.	REG_SZ	
BlockRecordingAnnotationFieldValue2		REG_SZ	
BlockRecordingAnnotationFieldValue3		REG_SZ	
BlockRecordingAnnotationFieldValue4		REG_SZ	
BlockRecordingAnnotationFieldValue5		REG_SZ	
PauseRecordingAnnotationFieldValue1	Specifies the field value that is tagged in Pause Recording command.	REG_SZ	
PauseRecordingAnnotationFieldValue2		REG_SZ	
PauseRecordingAnnotationFieldValue3		REG_SZ	
PauseRecordingAnnotationFieldValue4		REG_SZ	
PauseRecordingAnnotationFieldValue5		REG_SZ	
ResumeRecordingAnnotationFieldValue1	Specifies the field value that is tagged in Resume Recording command.	REG_SZ	""
ResumeRecordingAnnotationFieldValue2		REG_SZ	""
ResumeRecordingAnnotationFieldValue3		REG_SZ	""
ResumeRecordingAnnotationFieldValue4		REG_SZ	""
ResumeRecordingAnnotationFieldValue5		REG_SZ	""
EnableAnnotation Cleaning	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

Registry Entry	Description	Type	Default Value
ShowIcon	Set it to 1 to display the AIMTray icon on the task bar. Set it 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 it to 1.	REG_DWORD	1
ScreenOnlyWorkspace	**Applicable only in QM environments.** Set to 1 to allow anonymous login to a workspace without a telephone. When this option is selected, AIM sends a login event to the BDR Server when the session is opened and a logoff event when the session is closed.	REG_DWORD	0
HideExitMenuItem	Set this value to 1 to hide the Exit option in the AIMTray menu. 1 - Hide 0 - Display	REG_DWORD	0
AgentID	**Applicable only in QM environments.** Specifies the Agent ID to use in AIM messages.	REG_DWORD	0
Extension	**Applicable only in QM environments.** Specifies the Extension value to use in AIM messages.	REG_DWORD	0
HideLogonMenuItem	**Applicable only in QM environments.** Set this value to 1 to hide the Logon Agent option in the AIMTray menu. 1 - Hide 0 - Display	REG_DWORD	0
HideLogoffMenuItem	**Applicable only in QM environments.** Set this value to 1 to hide the Logoff Agent option in the AIMTray menu. 1 - Hide 0 - Display	REG_DWORD	0

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

Configurations Needed 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.

Read this section to understand all configurations required to enable agents to annotate calls from Agent Initiated Monitoring (AIM). These configurations are discussed in the following topics:

- Configure AIM to Support Annotations, page 124
- Configure Custom Attributes in Enterprise Manager, page 126
- Enable Custom Data Fields and Mapping Attributes, page 127
- Verify the Configuration is Working, page 128

Configure AIM to Support Annotations

Configuring AIM to support annotations is the first of four procedures associated with ensuring that agents can annotate calls with AIM.

This procedure 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.

To configure AIM to support annotations during the product installation, be sure to make the following configurations during the Screen Capture Module 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 can 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

NOTE For complete installation instructions, see "Screen Capture and AIM" on page 73.

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.

To configure these settings from the registry editor:

1 Start the registry editor on the computer on which the Screen Capture Module is installed (**Start > Run** and type **regedit**).

2 Open **HKLM\SOFTWARE\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).

Next procedure:

Configure Custom Attributes in Enterprise Manager**, page 126**

Configure Custom Attributes in Enterprise Manager

Configuring custom attributes in the Enterprise Manager application is the second of four procedures associated with ensuring that agents can annotate calls with AIM.

After you have provided values for the **User Field *X*** settings, as described in "Configure AIM to Support Annotations" on page 124, you must create custom attributes for each of the user fields.

The names of these custom attributes must *exactly* match the names that are specified for the **UserFieldName*X*** 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 **UserFieldName*X*** registry keys, as discussed in the procedure below.

1 The default values for each of the five **UserFieldName*X*** 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

NOTE 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. Navigate to **HKLM\SOFTWARE\Witness Systems\AIM** to view the registry keys.

2 Create custom attributes with names that exactly match the values associated with the **UserFieldName*X*** registry entries.

a. In the Enterprise Portal application, select **System Management > Custom Data > Attributes**.

b. Click 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. Click the **Save** button.

e. Repeat steps b., c., and 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 **Available Attributes** screen

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

Next procedure:

Enable Custom Data Fields and Mapping Attributes**, page 127**

Enable Custom Data Fields and Mapping Attributes

Enabling Custom Data fields for the Central Contact database and mapping attributes to the Custom Data fields is the third of four procedures associated with ensuring that agents can annotate calls with AIM.

After you have configured attributes in the Enterprise Manager, as described in "Configure Custom Attributes in Enterprise Manager" on page 126, you must enable five Custom Data fields and then map the attributes to those Data Fields. Follow the procedure below:

1 In the Enterprise Portal application, select **Organization Management > Recording, Quality Monitoring, and Analytics > Custom Data**.

2 Enable five Custom Data fields, one for each custom attribute that you configured in "Configure Custom Attributes in Enterprise Manager" on page 126. 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. Repeat step a. to enable the fields Custom Data 2 through Custom Data 5.

NOTE You can enable any five of the 25 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 **System Management > Custom Data > Custom Data**.

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" on page 126. For 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.

Verify the Configuration is Working

Verifying the configuration is working is the last of four procedures associated with ensuring that agents can annotate calls with AIM.

After performing the three previous procedures, annotate a call to verify the configuration is working.

To annotate a call:

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" on page 124. 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.

Troubleshooting 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.

In the Integration Service log, locate the IEMessage that contains the attributes of the AIM annotation message, and examine the attributes for errors.

In the audio call XML file, examine the <tag> attribute associated with the call annotation for possible errors.

Enabling 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`**, which resides at: **`HKEY_LOCAL_MACHINE\SOFTWARE\Witness Systems\eQuality Agent\Capture\CurrentVersion`**.

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 form the designated primary monitor screen.

Set the appropriate value for **`DualMonitor`** as needed.

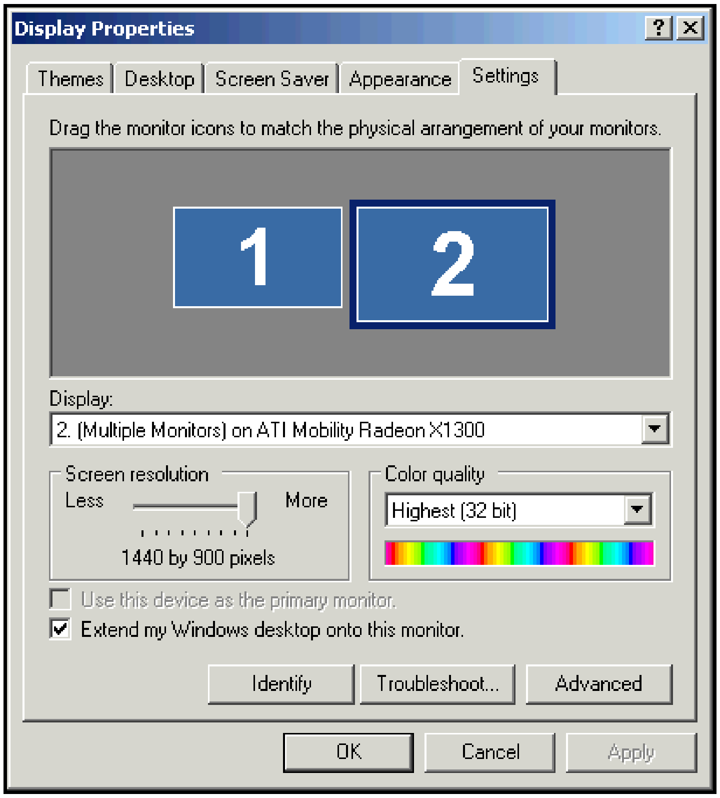
- Capturing video from multiple monitors increases the network bandwidth utilization.
- Monitors can have different resolutions. Recorded screen width will equal the sum of all monitor widths. Recorded screen height will equal the maximum height from all monitor heights.

NOTE

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 **Extend my Windows desktop onto this monitor** option in the Windows Display Properties dialog box.

If the monitors are attached to more than one display adapter then the behavior is unknown. In general, Screen Capture Module will capture all the monitors in sequence displayed in the Display Properties dialog.



Drag the monitor icons to match the physical arrangement of your monitors.

Display: 2. (Multiple Monitors) on ATI Mobility Radeon X1300

Screen resolution: 1440 by 900 pixels

Color quality: Highest (32 bit)

□ Use this device as the primary monitor.

☑ Extend my Windows desktop onto this monitor.

Known Issues

This section discusses Screen Capture Module configuration notes and known issues.

The Screen Capture Module known issues include:

Windows Vista Issues (Business and Enterprise Editions)

If the ‘Windows Aero’ color scheme is not enabled on the Agent workstation, then the Screen Capture Module may not be able to capture the Gadgets, Tooltips, and similar items displayed on the desktop.

This issue occurs only when the Screen Capture Module is installed on Windows Vista SP2 Business and Enterprise editions.

Windows Vista\Windows 7\Windows 2008 Terminal Server Issue

The following issue occurs when the Screen Capture Module is installed on the Windows Vista, Windows 7, and Windows 2008 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:
  a. In Windows Explorer, navigate to the **\Program Files\Witness Systems\Screen Capture Module** directory.
  b. Hover over the **LogManager.exe** and select **Run as Administrator** from the right-click menu.
- Using **regedit32**, give the user account that runs **LogManager.exe** full access to the **HKLM\SOFTWARE\Witness\Tracing** registry key.

Windows 7\Windows 2008 R2 Issues

The following issues occur when the Screen Capture Module is installed on the Windows 7 or Windows 2008 R2 Operating System, and the Windows User Account Control (UAC) settings are enabled:

- The LogManager.exe file must run as Administrator if you want to change the log settings. See "Windows Vista\Windows 7\Windows 2008 Terminal Server Issue" on page 131 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).

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 below:

1. Open the User Account Control settings using one of these methods:
   - **Start Menu > Control Panel > User Accounts and Family Safety > User Account**
   - **Start Menu > Control Panel > System and Security > Action Center**
2. Click or right-click on the Flag icon in the notification area (system tray), and select **Open Action Center**.
3. Type **`MsConfig`** in Start Search to start System Configuration.
4. Select the **Tools** tab, select **Change UAC Settings**, and then click the **Launch** button.
5. Select Change User Account Control settings.
6. Slide the slide bar down to the lowest value so that it is positioned at the **Never notify** setting.
7. Click OK.
8. 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.

For example, a black screen is recorded in the following 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 application 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:

1. Open Windows Media Player.
2. Select **Tools > Options**.
3. Select the **Performance** tab.
4. Click the **Advanced...** button.
5. In the Video Acceleration section, clear the check mark from the **Use overlays** setting.
6. Click **OK** in the Video Acceleration Settings window.
7. Click **Apply** and then click **OK** in the Options window.
8. Click **OK** in the Video Acceleration Settings window.
9. Click **Apply** and then click **OK** in the Options window.

Conserving Bandwidth Usage and Disk Storage Space 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.

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, by adjusting 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.

An Upgrades Does 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.

System Administrators can change the ColorReduction setting in the registry by opening the registry editor and navigating to the following parameter:

```
HKEY_LOCAL_MACHINE\SOFTWARE\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.

For example, 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.

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.

This chapter includes:

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.

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 machine. 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 was added to eliminate privacy concerns within your organization. It can be disabled with the help of customer support.

CapTestB System Requirements

CapTestB is supported on the following operating systems:

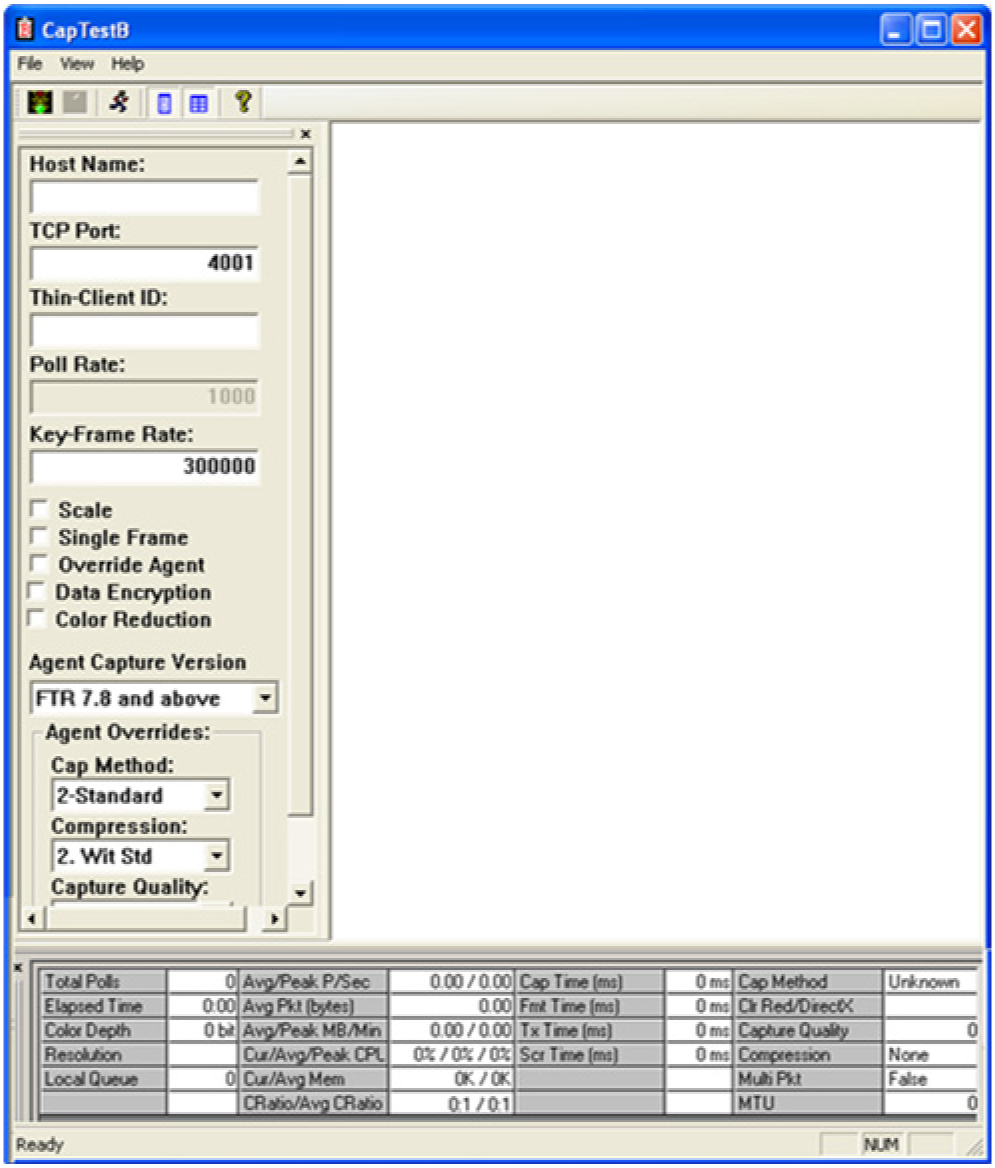
- Windows 7 32/64 bit
- Windows Vista
- Windows XP Professional
- Windows Server 2003 32/64 bit
- Windows Server 2008 32/64 bit

Running the CapTestB Utility

1. Copy the **Captest.zip** file to a machine 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 it fails to run, install the **vcredist_x86.exe** application file that was included in the Captest.zip and then run **captest.exe** again.

   The CapTestB Utility opens to the main window. The CapTestB main window contains a control bar (left frame), statistics grid (lower frame) and playback window for viewing screen captures.



Host Name:

TCP Port: 4001

Thin-Client ID:

Poll Rate: 1000

Key-Frame Rate: 300000

□ Scale
□ Single Frame
□ Override Agent
□ Data Encryption
□ Color Reduction

Agent Capture Version: FTR 7.8 and above

Agent Overrides:

Cap Method: 2-Standard

Compression: 2. Wit Std

Capture Quality:

Total Polls	0	Avg/Peak P/Sec	0.00 / 0.00	Cap Time (ms)	0 ms	Cap Method	Unknown
Elapsed Time	0:00	Avg Pkt (bytes)	0.00	Fmt Time (ms)	0 ms	Clr Red/DirectX	
Color Depth	0 bit	Avg/Peak MB/Min	0.00 / 0.00	Tx Time (ms)	0 ms	Capture Quality	0
Resolution		Cur/Avg/Peak CPL	0% / 0% / 0%	Scr Time (ms)	0 ms	Compression	None
Local Queue	0	Cur/Avg Mem	0K / 0K			Multi Pkt	False
		CRatio/Avg CRatio	0:1 / 0:1			MTU	0

4 Configure the control bar with test parameters and agent workstation parameters.

See Control Bar, page 138

5 Select **File > Start Monitor** or click the Start button on the toolbar.

In most configurations, an alert appears on the workstation informing the user that the utility is attempting to monitor the workstation. Click **OK**.

Screen Capture performance statistics appear in the Statistics Grid. See Statistics Grid, page 139 for a description of each statistic.

6 Analyze screen capture performance. The performance statistics are color coded to reflect threshold and danger levels.

See Analyzing Performance, page 139

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.

CapTestB Configuration Parameters:

- **Host Name:** host name of the agent's PC or the host name of a thin-client server.
- **TCP Port:** TCP connection port number. 4001 for workstations and 4002 for thin-client servers.
- **Thin-Client ID**: the 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 PC 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 of captured screen files are encrypted.
- **Color Reduction:** Select to reduce captured color to 8-bit (256 colors).

Agent Workstation Screen Capture Parameters:

- **Agent Capture Version:**
- **Capture Method:** Desired detection method: 1=Enhanced, 2=Standard.
- **Capture Quality:** Desired capture quality setting from 1 to 10.
- **Compression:** Desired compression method: 1=Witness Enhanced, 2=Witness Standard, 3=MSRLE8, 4=JPEG, 5=5.x Compatibility, 6=6.3 Compatibility, 7=dynamic
- **Compression Quality:** Desired compression quality setting from 1 to 10.

Statistics Grid

The following performance statistics are reported in the statistics grid:

- **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 machine.
- **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.
- **Curr/Avg/Peak Rem CPU**: the current, average, and peak CPU usage by WCapW32.exe on the agent's machine.
- **Curr/Avg Rem Mem**: the current and the average memory usage by WCapW32.exe on the agent's machine.
- **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 machine 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 machine.
- **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 machine.
- **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 machine.

Analyzing Performance

Performance analysis involves gathering statistics for different configuration sets and selecting the most optimal settings for the given environment. There are typically three objectives to choose from:

- Agent impact
- Recording quality
- Journal-file size.

The choices you make will favor one of these. 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.

Several of the statistics have been assigned warning and danger threshold values. If measurements exceed these thresholds, the background color of the grid cell will be changed to yellow or red. The statistics and their threshold values are listed in the table below.

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, you must strive to stay below warning thresholds. In extreme cases, this may not be possible, and you may have to sacrifice performance. In any case, a careful analysis of statistics gathered will help you determine the most optimal settings as well as problem areas within the recording environment.

Appendix B

Media Encoder

Media Encoder

Using the Media Encoder, it is possible to convert audio files to a PCM-encoded .wav format for machines inside or outside the organization that are not installed with the Playback application and/or cannot access the Portal.

Installation Prerequisites

Microsoft .NET Framework 2.0 or higher is required.

Installing the Media Encoder

- Install Playback. Installing Playback automatically installs the Media Encoder. See "Playback" on page 63.

  The Media Encoder is installed in this location: **C:\Program Files\<Company Name>\Playback\CommandLineConvertor**

Converting Audio Files

You can convert audio files to the PCM-encoded .wav format either from 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 machine that does not have Playback or the proprietary compressed codec installed.

NOTE The Media Encoder does not support the conversion of encrypted files.

- Enabling the Convert Option, page 142
- Disabling the Convert Option, page 143
- Converting from the Command Line, page 143

Enabling the Convert Option

This is relevant for machines running Windows Operating Systems only.

1. Open a text editor (e.g. 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\&Verint_convert]
```

```
@="&Verint_convert"
[HKEY_CLASSES_ROOT\SoundRec\shell\&Verint_convert\command]
@="\"C:\\Program Files\\Verint\\Playback\\CommandLineConvertor.exe\" \"%L\""
```

3 If Playback 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 **Verint convert** option appears when you right-click an audio file.

NOTE Verint 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 machine that does not have Playback/Verint Codec installed.

Disabling the Convert Option

To disable the convert right-click option in Windows menus:

1 Run the following command: `CommandLineConvertor -UnRegShell`

2 Verify that the **Verint convert** option does not appear in the menu when you right-click an audio file.

Converting from the Command Line

- Run the following command:

  `cd [Path to the Media Encoder application file] CommandLineConvertor [inputFileName] [outputFileName]`

  The parameters are described in following table:

Parameter	Description
Path to the Media Encoder application file	C:\Program Files\<company name>\Playback (default installation location)
CommandLineConvertor	Media Encoder application file name
inputFileName	Full path and name of the audio file you want to convert

Parameter	Description
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

For Example:

```
cd C:\Program Files\<company name>\Playback CommandLineConvertor
C:\My Media Files\originals\input.wav C:\My Media
Files\converted\output.wav
```

You can now send the converted output file to machine that does not have Playback/Verint Codec installed.

Installing V11 SP1 Agent Workstations for Acquisition Recording

Agent Desktop Applications for Acquisition Recording

This appendix is relevant in upgrade scenarios from ULTRA 9 or Impact 360 V10 only, and is part of a larger upgrade workflow. See "Upgrading from ULTRA 9 or Impact 360 V10" on page 91.

The Desktop Applications required on the workstations of users defined as Agents in an Acquisition Recording environment are listed in the following table:

Agent Desktop Applications	
Record On-Demand for Acquisition Recording	The Record On Demand desktop application enables agents to control call recordings (for example, start, stop or mute a recording), and perform data tagging directly from the agent's desktop.
Screen Capture for Acquisition Recording	Screen Recording records agent screen activity both during the interaction between an agent and the contact center customer and for a configurable amount of wrap up time after the contact has ended. It is activated based on configurable recording rules. By default, screens are recorded only for a percentage of contacts.
CTI Link Agent	CTI Link Agent is installed on each agent desktop to provide agent identification in a free-seating environment and to provide screen recording information to the Acquisition Integration Service server role. Mapping the agent PC to a phone extension based on the agent's network login achieves agent identification.
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.

The predefined Agent role does not have access to the Portal. If agents are granted access, then **Playback** is required.

Manually Installing Agent Workstations for Acquisition Recording

The following are the manual installation instructions for the agent workstations compatible with acquisition recording.

- Installing Record on Demand, page 147
- Installing Screen Capture for Acquisition Recording, page 148
- Installing CTI Link Agent, page 150
- Installing Logger, page 153

Installing Record on Demand

The Record On-Demand desktop application is installed **only when agents are required to control call recordings** (for example, start, stop or mute a recording), and perform data tagging directly from the agent's desktop.

When recording control APIs are available to performthese tasks without agent intervention, an Impact 360 SDK license is required.

1. Run the **RODInstallation.msi** file.

   The **Welcome** screen of the setup wizard appears.
2. Click **Next**.

   The **End-User License Agreement** screen appears.
3. Select **I accept the terms in the License Agreement** and click **Next**.

   The **Custom Setup** screen appears.

   To view the required space for an application, select it in the list and read the text in the pane on the right.
4. 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** screen appears.
6. Enter the **HTTP/HTTPS Alias** of the Application Server.

   Resolve the HTTP/HTTPS Alias alias by browsing to the Impact 360 Portal Enterprise Settings and selecting the **Consolidated or Application Server > Additional Settings > HTTP/HTTPS Alias.**.
7. (Optional) Select **Use SSL for client/server communication**.
8. Click **Next**.

   The **Record-on-demand Settings** screen appears.

9 Type the **HTTP/HTTPS Alias** of the Acquisition Recorder server associated with the Acquisition Integration Service Server Role.

Resolve the HTTP/HTTPS Alias by browsing to the Impact 360 Portal Enterprise Settings and selecting the **Acquisition Recorder Server > Additional Settings > HTTP/HTTPS Alias**.

10 In the **Extension** field, type the workstation extension.

11 Type caption names for the three data fields that can be updated from the Record On Demand application.

These captions will appear in the Record On Demand application only. For other Impact 360 V11 applications, the field names are defined in the Caption Editor. These three fields are mapped to Custom Data 1, 2, and 3 respectively, unless changed during upgrade from previous versions.

12 Specify the functionality to be available in the Record On Demand application by selecting the relevant check boxes, and then click **Next**.

The **Ready to Install** window appears.

13 Click **Install**.

When the installation is complete, the **Installation Success** window appears.

14 Click **Finish** to exit the installation wizard.

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

15 Restart your computer.

Language Settings

To view the Record On-Demand application interface in a language other than English, set your regional settings for non-unicode programs to the required language.

To change the regional settings:

1 From the **Start** menu, select **Settings > Control Panel > Regional and Language Options**.

The Regional and Language Options screen is displayed.

2 In the **Advanced** tab, in the **Language** list, select the required language and click **OK**.

Installing Screen Capture for Acquisition Recording

Install screen capture, and then configure the recommended screen capture settings.

1 Run the **ScreenRecording.msi** file.

The **Welcome** screen of the setup wizard appears.

2 Click **Next**.

The **End-User License Agreement** screen appears.

3 Select **I accept the terms in the License Agreement** and click **Next**.

The **Custom Setup** screen appears.

To view the required space for an application, select it in the list and read the text in the pane on the right.

4 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 **Screen Recording Settings** screen appears.

6 If required, change the default **Recording Method** and **Encoding Level** settings.

7 For operating systems (other than Windows Vista, Windows 7 and Windows 2008) that support personal firewalls, select **Open ports for screen recording**, and then click **Next**.

If this check box is not selected, you will need to manually open port 5600 on the computer firewall later. On Windows Vista, Windows 7 and Windows 2008 operating systems, this port cannot be opened during the Desktop installation and needs to be opened manually.

The **Ready to Install** window appears.

8 Click **Install**. The **Updating System** window opens.

9 Wait while the features are installed. When the installation is complete, the **Installation Success** window appears.

10 Click **Finish** to complete the installation.

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

11 Restart your computer.

12 Continue to **Acquisition Screen Capture Settings**.

Acquisition Screen Capture Settings

The following settings are required or recommended:

- To increase workstation performance during screen recording, it is recommended that all Acquisition Agent workstations are configured to use 16-bit color settings rather than 32-bit color settings.
- It is recommended to remove any background on the agent workstation desktops.

  To configure the desktop background, select **Start > Settings > Control Panel > Display > Background**.

  The background increases the size of the screen files and consequently, network traffic and CPU consumption is also increased.
- Adjust the mouse pointer properties as follows

  a. From the **Start** menu, select **Settings > Control Panel > Mouse > Pointers** tab.

b. Ensure the mouse pointer Scheme is set to **None**.

c. In Windows 2000, ensure that the **Enable Pointer Shadow** option is disabled.

Installing CTI Link Agent

1 Run the **ILA.msi** file. The **Welcome** screen of the setup wizard appears.

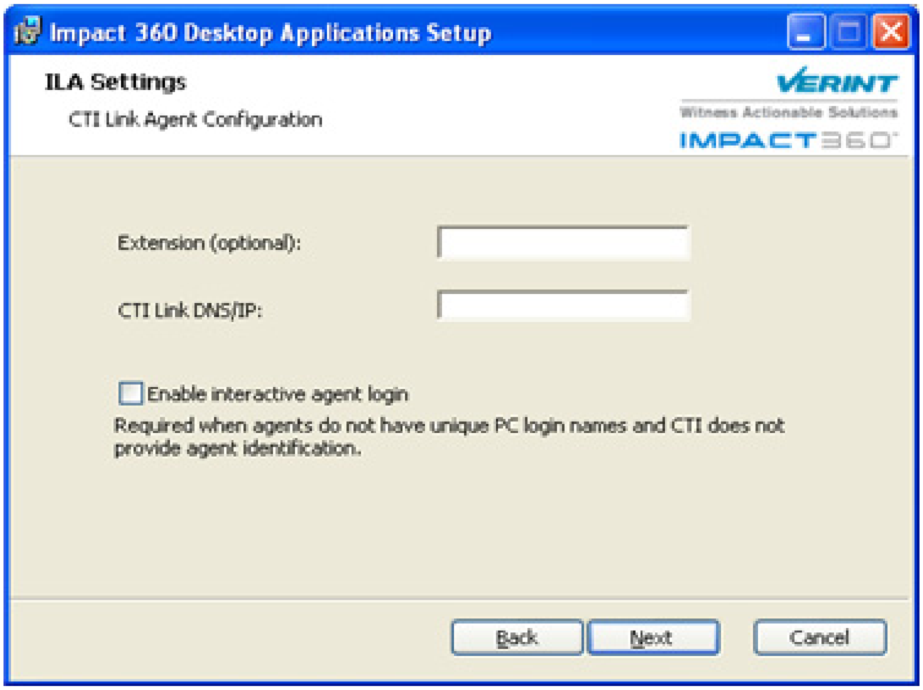
2 Click **Next**. The **End-User License Agreement** screen appears.

3 Select **I accept the terms in the License Agreement** and click **Next**. The **Custom Setup** screen appears.

To view the required space for an application, select it in the list and read the text in the pane on the right.

4 Click **Next**. If a list of missing prerequisites appears, click **Close** and then **Cancel**. Install the missing prerequisites and restart the installation.

When there are no missing prerequisites, the **ILA Settings** screen appears.


Impact 360 Desktop Applications Setup
ILA Settings
CTI Link Agent Configuration
VERINT
Witness Actionable Solutions
IMPACT360
Back
Next
Cancel

Extension (optional):

CTI Link DNS/IP:

□ Enable interactive agent login

Required when agents do not have unique PC login names and CTI does not provide agent identification.

5 (Optional) In the **Extension (optional)** field, type a numeric phone extension for the agent. The **Extension (optional)** field is not required if you are installing in a Citrix or Network Server environment.

6 In the **CTI Link DNS/IP** field, type the **HTTP/HTTP Alias** of the server associated with the Acquisition Integration Service server role.

Resolve the HTTP/HTTPS Alias by browsing to the Impact 360 Portal Enterprise Settings and selecting the **Acquisition Recorder or Consolidated Server > Additional Settings > HTTP/HTTPS Alias**.

7 Select **Enable interactive agent login** if agents do not have unique PC login names and CTI does not provide agent identification, and then click **Next**.

NOTE If you are using **Citrix Published Application** mode and are installing the **CTI Link Agent** application, you can enable a seamless startup and log off for this application. See **Enabling Seamless Startup and Logoff for CTI Link Agent** for more information.

The **Ready to Install** window appears.

8 Click **Install**.

When the installation is complete, the **Installation Success** window appears.

9 Click **Finish** to exit the installation wizard.

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

10 Restart your computer.

11 Continue to the following procedures if relevant:

- Configuring CTI Link Agent to Work with Multiple Switches, page 151
- Updating CTI Link IP address in the CTI Link Agent Configuration, page 151
- Enabling Seamless Startup and Logoff for CTI Link Agent in a CItrix Environment, page 152

Configuring CTI Link Agent to Work with Multiple Switches

When workstations require to work with multiple switches so that agents can log into more than one switch (at different times), the CTI Agent application must be able to communicate with multiple instances of CTI Link.

Note that in Citrix Server environments, all agents that log into this server will be defined with the same set of CTI Link servers.

The following application is only available after CTI Agent installation on the agent desktop.

Updating CTI Link IP address in the CTI Link Agent Configuration

It is required to perform this procedure whenever an IP address of the Acquisition Recorder hosting CTI Link is removed, added, or modified .

1 Log in to the workstation as a user with administrative rights. For workstations installed with Windows Vista/7/2008 Operating Systems, elevate the UAC security in order 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**.

2 If prompted for the user name and password, provide administrator credentials.

3 Browse to **C:\Program Files\Verint\ILA** and double-click the **ILAUpdateILIP.exe** file. The CTI Link Server IP Update dialog box appearsdisplaying the IP address currently configured.

4 Click **Add New IL IP**.

5 Enter the DNS and click **Save**.

Enabling Seamless Startup and Logoff for CTI Link Agent in a CItrix Environment

Customers who use the **Citrix Published Application** mode and who installed the **CTI Link Agent** application need to update their system processes to enable CTI Link Agent to seamlessly start and close.

The update includes changing registry keys and must be performed on each Citrix server after the Impact 360 Desktop installation. Follow the relevant procedure according to the installed features:

To enable seamless startup and logoff for CTI Link Agent

1 From the Impact 360 Installation CD, from the **Tools\Citrix** folder, open the **Citrix.zip** and copy **IlaApp.cmd** to the **%WINDIR%\system32** folder.

2 Via Notepad, open **UltraApp.cmd** and verify that the directory path points to the CTI Link Agent installation path. If not, modify the path accordingly.

3 Configure Anti-Virus not to remove IlaApp.cmd.

4 Run **IlaApp.cmd** and verify that the **ILALoginApp**, **RFBAgent.exe** and **HostedApp** processes appear in the Windows Task Manager; then end the processes.

5 From the Impact 360 Installation CD, from the **Tools\Citrix** folder, open the **Citrix.zip** and run **InstallILAforsharedapp.vbs** to update the following registry keys:

- **HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\App Setup**
- **HKLM\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI\LogoffCheckSysModules**

These updates add **RFBAgent.exe** and **Ilaloginapp.exe** to the list of executables that seamlessly start upon a user's login and terminate upon logoff, thus ensuring the proper functioning of the CTI Link Agent.

6 Export the following registry key: **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ILA** (for rollback purposes).

7 Delete the following registry key: **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ILA**.

8 Verify the updates as follows:

a. On a Citrix client with no open session, run one of the published applications.

b. On the Citrix server, check the session information and verify that the **RFBAgent.exe** and **ILALoginApp**, processes appear in the Windows Task Manager.

c. From the same Citrix client session, run a second published application.

d. On the Citrix server, look at the session information and verify that the **RFBAgent.exe**, and **ILALoginApp** processes do not appear twice in the Windows Task Manager.

e. On the client side, close the second application.

f. On the Citrix server, verify that the session does not end on the Citrix server side and that CTI Link Agent and RFB continue running.

g. On the client side, close the first application and verify that the session ends on the Citrix side and CTI Link Agent and RFB stop running.

Installing Logger

1 Run the **LoggerInstallation.msi** file.

The **Welcome** screen of the setup wizard appears.

2 Click **Next**.

The **End-User License Agreement** screen appears.

3 Select **I accept the terms in the License Agreement** and click **Next**.

The **Custom Setup** screen appears.

To view the required space for an application, select it in the list and read the text in the pane on the right.

4 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** window appears.

6 Click **Install**.

When the installation is complete, the **Installation Success** window appears.

7 Click **Finish** to exit the installation wizard.

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

8 Restart your computer.

Silently Distributing Agent Workstations for Acquisition Recording

This section provides both an example script for silent distribution and a list of relevant command line parameters for the default user.

Create an installation script for the workstation based on the example and modify the parameter default values as required for your specific deployment.

IMPORTANT Silent installation parameters are case sensitive and are required to be capitalized.

- Example Script for Agents with Acquisition Recording, page 154
- Silent Install Parameters for Agent workstations with Acquisition Recording, page 155

Example Script for Agents with Acquisition Recording

This script is an example for silently installing the following applications: Logger, Record On-Demand, Screen Capture for Acquisition Recording and CTI Link Agent.

```
@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 sucessfully
REM If installation fails, the EXIT_CODE is 1
 set MSIS_DIR=\\<Shared network folder:>\Impact360_DesktopApplications
set VERINTFOLDER=C:\Program Files\Verint
SET EXIT_CODE=0
echo Logger Installation
msiexec -i "%MSIS_DIR%\LoggerInstallation.msi" USE_COMMAND_LINE=1
VERINTFOLDER="%VERINTFOLDER%" /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
)  ELSE    (
echo ---installer succeded
)
echo Record on-Demand
 msiexec -i "%MSIS_DIR%\RODInstallation.msi" USE_COMMAND_LINE=1 VERINTFOLDER="%VERINTFOLDER%"
ROD_CFM_DNS=LMAcq ROD_DATA1="First"  ROD_DATA2="Second" ROD_DATA3="Third"
ROD_EXTENSION=7777777 ROD_MUTE=1 ROD_ROD=1 ROD_SOD=1 /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
)  ELSE    (
echo ---installer succeded
)
echo Screen Recording
msiexec -i "%MSIS_DIR%\ScreenRecording.msi" USE_COMMAND_LINE=1 VERINTFOLDER="%VERINTFOLDER%"
SRA_ENCODING=3 SRA_OPENFIREWALLPORTS=1 SRA_POLLFULLSCREEN=0 /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
)  ELSE    (
echo ---installer succeded
)
echo CTI Link Agent
msiexec -i "%MSIS_DIR%\ILA.msi" USE_COMMAND_LINE=1 VERINTFOLDER="%VERINTFOLDER%"
ILA_EXTENSION=7777777 ILA_INFOLINKIP=LMAcq /qn
IF %errorlevel% NEQ 0 (
SET /A EXIT_CODE=1
echo ---installer failed
)  ELSE     (
 echo ---installer succeded
)
echo EXIT_CODE is %EXIT_CODE%
exit /B %EXIT_CODE%
```

Silent Install Parameters for Agent workstations with Acquisition Recording

The following mandatory and configurable parameters are for the default Desktop Applications required for Agent workstations with Acquisition Recording:

- General Install Parameters, page 155
- Record On Demand Silent Install Parameters, page 156
- Screen Capture for Acquisition Recording Silent Install Parameters, page 157
- CTI Link Agent Silent Install Parameters, page 157
- Logger Silent Install Parameters, page 158

General Install Parameters

The following general parameters are required to be set:

General Parameters	Description and Default Values
MSIS_DIR	Specifies the location of shared folder defined to save the installation files. **Default:** <Shared network folder:>\Impact360_DesktopApplications
VERINTFOLDERt	Specifies the installation destination. **Default:** C:\Program Files\Verint

Record On Demand Silent Install Parameters

The following properties determine how Record on-Demand is configured silently on the agent desktops.

Basic Parameters	Description and Default Values
USE_COMMAND_LINE	USE_COMMAND_LINE=1 **Mandatory**
ROD_CFM_DNS	The DNS or IP address of the CFM (Acquisition Director) server.
ROD_DATA1	Custom Data CD1 field default value. **Default = Empty**
ROD_DATA2	Custom Data CD2 field default value. **Default = Empty**
ROD_DATA3	Custom Data CD3 field default value. **Default = Empty**
ROD_EXTENSION	The extension to use with ROD. **Mandatory**
ROD_MUTE	0 = Disable the mute feature. 1 = Enable the mute feature. **Mandatory ROD_MUTE=1**
ROD_ROD	0 = Disable the Record On Demand feature. 1 = Enable the Record On Demand feature. **Mandatory ROD_ROD =1**
ROD_SOD	0 = Disable the Stop On Demand feature. 1 = Enable the Stop On Demand feature. **Mandatory ROD_SOD =1**

Screen Capture for Acquisition Recording Silent Install Parameters

The following properties determine how Screen Capture for Acquisition Recording is configured silently on the agent desktops.

Basic Parameters	Description and Default Values
USE_COMMAND_LINE	USE_COMMAND_LINE=1 **Mandatory**
SRA_ENCODING	Specifies the encoding level. 1 = Low 2 = Medium 3 = High
SRA_OPENFIREWALLPORTS	0 = Do not open firewall port. 1 = Open firewall port.
SRA_POLLFULLSCREEN	Specifies the recording method. 0 = Standard 1 = Full screen

CTI Link Agent Silent Install Parameters

The following properties determine how CTI Link Agent is configured silently on the agent desktops.

Basic Parameters	Description and Default Values
USE_COMMAND_LINE	USE_COMMAND_LINE=1 **Mandatory**
ILA_EXTENSION	The extension to use with CTI Link Agent (ILA). **Default = Empty**
ILA_INFOLINKIP	The HTTP/HTTPS Alias of the server hosting the Acquisition Integration Service. **Mandatory**
ILA_INFOLINKIP1 to ILA_INFOLINKIP8	The HTTP/HTTPS Alias of the servers hosting the Acquisition Integration Services (numbered 1 to 8). **Default = Empty**

Logger Silent Install Parameters

The following 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**
VERINTFOLDER	%VERINTFOLDER%

Appendix D

Related Documentation

The following table lists the relevant administration and user guides for each desktop application.

Desktop Application	**Guide Name**
Screen Capture with AIM	*AIM Quick Reference Guide*
Playback	*Interactions for Supervisors/Agents User Guide*
Form Designer Standalone Form Designer	*Quality Monitoring Form Designer User Guide* *Standalone Form Designer Installation Guide*
Pop-up Notification System Client	*Workforce Management Administration Guide* *Workforce Management Schedulers' Guide* *Workforce Management Managers' Guide* *Workforce Management Agents Guide*
Content Producer	*Content Producer Installation and Upgrade Guide* *Content Producer User Guide*
Forecasting and Scheduling	*Workforce Management Schedulers' Guide*
Strategic Planner	*Workforce Management Planners' Guide*
Phonetics Boosting	*Phonetics Boosting User Guide*
Real Time Speech Calibration Application	*Real Time Speech Calibration Application User Guide*
Desktop Gadgets	*Scorecards User Guide* *Scorecards Administration Guide*
Desktop and Process Analytics (DPA) Client DPA Process Discovery	*Desktop and Process Analytics (DPA) User Guide* *Desktop and Process Analytics (DPA) Installation and Configuration Guide*

Verint Global Headquarters
330 South Service Road
Melville, NY 11747 USA

info@verint.com
1-800-4VERINT

www.verint.com