Cloud Contact Center
Software

Technical Requirements

Reference Guide

August 2021

This guide contains deployment, configuration, and troubleshooting information to assist customers and partners with Five9 applications.

About Five9

Five9 is the leading provider of cloud contact center software, bringing the power of the cloud to thousands of customers and facilitating more than three billion customer interactions annually. Since 2001, Five9 has led the cloud revolution in contact centers, delivering software to help organizations of every size transition from premise-based software to the cloud. With its extensive expertise, technology, and ecosystem of partners, Five9 delivers secure, reliable, scalable cloud contact center software to help businesses create exceptional customer experiences, increase agent productivity and deliver tangible results. For more information visit www.five9.com.

Trademarks

Contents

What's New

This table lists the changes made in the last six releases of this document:

Release	Changes
August 2021	• Added Five9 IP Addresses for Callback API Integration. • Added inbound SFTP port in TCP Port Requirements for FTP/SFTP. • Updated Clearview domains list in Performance Dashboard. • Updated Java Runtime Environment support information to 1.8.0_301 32-bit. • Removed Five9 NAT IP Addresses section.
July 2021	• Added Five9 domains for US, CA, and EU regions in Five9 Internet Domains. • Added Five9 NAT IP Addresses section in Five9 Internet Domains and IP Addresses. • Added Studio Requirements . • Removed Windows 7 support.
June 2021	• Added Edge browser support: ◦ Updated Web Browsers in Web-Based Application Requirements ◦ Updated Web Browsers in Workstation Requirements for Five9 Video Engagement ◦ Updated Web Browsers in Requirements for Web-Based Adapters • Added Workforce Optimization Requirements. • Updated Java Runtime Environment support information to 1.8.0_291 32-bit.
May 2021	• Added bandwidth requirements for RingCentral in Five9 Bandwidth Requirements. • Added MacOS Big Sur support: ◦ Updated Workstations, Operating Systems, Web Browsers in Web-Based Application Requirements ◦ Updated Workstations, Operating Systems, Web Browsers in Workstation Requirements for Five9 Video Engagement ◦ Updated Workstations, Operating Systems, Web Browsers in Requirements for Web-Based Adapters ◦ Updated Operating Systems, Web Browsers in Requirements for Java-Based Adapters ◦ Added a note about MacOS Big Sur and Safari 14 in Java-Based Application

Release	Changes
	Requirements • Updated Java Runtime Environment Support information to 1.8.0_281 32-bit. • Updated IP address ranges for US, Canada, and EU data centers in Five9 IP Address Ranges. • Updated Port Requirements for Email. • Updated Five9 Connectivity Assessment Test. • Updated bandwidth requirements for Teams, Zoom, and Office@Hand in Five9 Bandwidth Requirements. • Moved IP addresses information from Verint Systems Requirements to Five9 IP Address Ranges. • Moved workstation, browser, and operating systems information from WebRTC to Web-Based Application Requirements.
April 2021	• Updated Verint Systems Network Requirements (LAN and WAN) and Workstation Requirements. • Removed note about disabling *Throttle JavaScript timers in background* in the Chrome browser.
March 2021	• Added Five9 IP Addresses for Email. • Added Five9 Agent Assist Requirements. • Added URL for Office@Hand in Five9 Internet Domains. • Added Agent Assist and Office@Hand bandwidth requirements in Five9 Bandwidth Requirements. • Updated Digital Certificates • Updated workstation recommendations in WebRTC.

Environment and Security

Important

Before configuring your organization, be sure to obtain the most current security and legal information relevant to your business. For example, you can start by consulting the Five9 Enterprise-Ready Security pages and your legal advisor.

RMI Protocol

Five9 uses the secure Remote Method Invocation (RMI) protocol for the Java-to-Java communications between the Five9 client applications and Virtual Contact Center platform. The RMI traffic is transmitted out of the firewall through open TCP ports by using the TLS protocol.

RTP Protocol

Voice traffic for VCC is transferred using the Real-Time Transport Protocol (RTP). The RTP download (*inbound*) streams the voice packets sent from the Five9 data center to the agent's softphone. The voice packets that represent the caller's voice upstream (*outbound*) are rebuilt in the softphone. The voice packets are sent from the agent's softphone to the Five9 data centers to be rebuilt and played back to the caller as the agent's voice. The voice packet transfer uses User Datagram Protocol (UDP) which is faster and more efficient than TCP for time-sensitive applications, such as VoIP. Intercepting the RTP stream to listen in on a leg of the call would require local network access to successfully rebuild the packets into an intelligible voice stream.

Voice Quality Testing

Five9 Connectivity Assessment Test (CAT) uses Port 80 and 8081. You can run VoIP quality tests at https://www.five9.com/cat from a single agent workstation at each location. Do not run multiple tests simultaneously.

Digital Certificates

To communicate securely with Five9 VCC, users may need to install on their workstation these certificates from the certificate-issuing authorities that Five9 uses.

Important

Following industry best practices and certificate authorities (CA), Five9 will no longer trust or certify secure TLS connections based on the certificates issued by Symantec Root Certificate Authority (CA) listed below. If you do not replace these distrusted certificates, your Five9 integration may not work. Therefore, Five9 highly recommends that you replace the distrusted certificates with the certificates issued by DigiCert.

Five9 will no longer trust the following Symantec Root CAs:

- CN=GeoTrust Global CA, O=GeoTrust Inc., C=US
- CN=GeoTrust Primary Certification Authority, O=GeoTrust Inc., C=US
- CN=GeoTrust Primary Certification Authority - G2,
  OU=(c) 2007 GeoTrust Inc. - For authorized use only, O=GeoTrust Inc., C=US
- CN=GeoTrust Primary Certification Authority - G3,
  OU=(c) 2008 GeoTrust Inc. - For authorized use only, O=GeoTrust Inc., C=US
- CN=GeoTrust Universal CA, O=GeoTrust Inc., C=US
- CN=thawte Primary Root CA, OU="(c) 2006 thawte, Inc. - For authorized use only",
  OU=Certification Services Division, O="thawte, Inc.", C=US
- CN=thawte Primary Root CA - G2, OU="(c) 2007 thawte, Inc. - For authorized use only",
  O="thawte, Inc.", C=US
- CN=thawte Primary Root CA - G3, OU="(c) 2008 thawte, Inc. - For authorized use only",
  OU=Certification Services Division, O="thawte, Inc.", C=US
- EMAILADDRESS=premium-server@thawte.com, CN=Thawte Premium Server CA,
  OU=Certification Services Division, O=Thawte Consulting cc,
  L=Cape Town, ST=Western Cape, C=ZA

- OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only",
  OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
- OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
- OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only",
  OU=Class 3 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
- CN=VeriSign Class 3 Public Primary Certification Authority - G3,
  OU="(c) 1999 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network,
  O="VeriSign, Inc.", C=US
- CN=VeriSign Class 3 Public Primary Certification Authority - G4,
  OU="(c) 2007 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network,
  O="VeriSign, Inc.", C=US
- CN=VeriSign Class 3 Public Primary Certification Authority - G5,
  OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network,
  O="VeriSign, Inc.", C=US
- CN=VeriSign Universal Root Certification Authority,
  OU="(c) 2008 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network,
  O="VeriSign, Inc.", C=US

DigiCert Certificates

Certificate	Link
High Assurance EV Root CA	https://cacerts.digicert.com/DigiCertHighAssuranceEVRootCA.crt.pem
Global Root CA	https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem

Supported TLS Protocols

Five9 does not accept unencrypted API connections. When developing a custom web service to communicate with the Five9 API, ensure that your web service uses these security protocols and that you use the web browsers versions supported by Five9. If

your environment uses proxy servers, these must support the secure WebSocket (WSS) protocol for desktop and network proxies.

Security Protocol	Notes
TLS	Transport Layer Security protocol. TLS 1.2 and TLS 1.1 are supported for inbound and outbound traffic.
TLS Cipher Suite	Minimum of 128-bit encryption is required.
WSS	Secure WebSocket (WSS) protocol uses TLS encryption.
Diffie-Hellman Key	Must be greater than or equal to 2048.

TLS Inbound Cipher Suites

The following are the supported TLS inbound cipher suites. To verify that your servers support these ciphers, go to SSL Server Test.

TLS 1.2 Inbound Cipher Suites

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

TLS 1.1 Inbound Cipher Suites

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

TLS Outbound Cipher Suites

The following are the supported TLS 1.2 outbound cipher suites. To verify that your servers support these ciphers, go to SSL Server Test.

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)

- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Setting the TLS Protocols in Your Browser

Enable TLS 1.1 and TLS 1.2 encryption protocols in your browser security settings.

Important

Follow these steps only if instructed to do so by your administrator.

Chrome

1. Open Chrome.
2. On your keyboard, press **Alt F** and select **Settings**.
3. At the bottom of the page, click **Advanced**.
4. Scroll down to the **System** section and click **Open proxy settings**.

5 From the **Internet Properties** menu, select the **Advanced** tab.
6 In the **Security** section, enable **Use TLS 1.1** and **Use TLS 1.2**.
7 Click **Apply** and **OK**, and restart Chrome.

Firefox

1 In the Firefox address bar, type **about:config** and press **Enter**.
2 Click **Accept the Risk and Continue**.
3 In the search field, type **tls**.
4 From the search results, double-click **security.tls.version.min**.
5 For TLS 1.1, enter **2**.
6 Click **OK**.
7 Close the tab, and restart Firefox.

Apple Safari

TLS 1.1 and TLS 1.2 are automatically enabled in version 9 or greater.

Internet Explorer

1 Click the **Tools** gear icon near the top right corner, and select **Internet options**.
2 Select the **Advanced** tab.
3 Scroll to the end of the list, and enable **Use TLS 1.1** and **Use TLS 1.2**.
4 Click **OK**, and restart Internet Explorer.

Five9 SIP Trunk Options

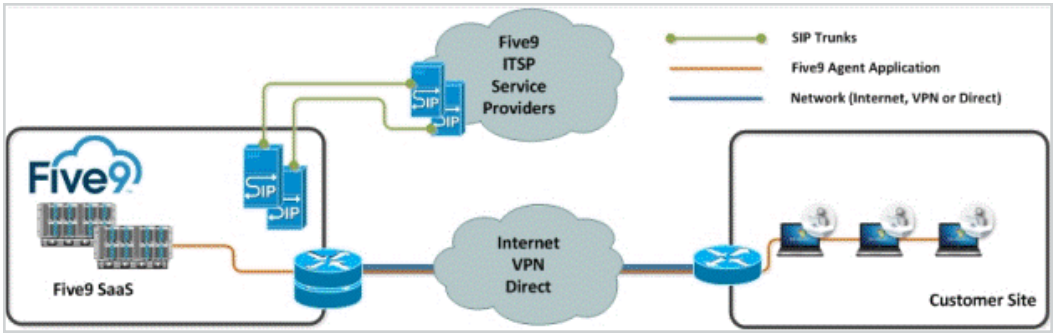
SIP trunks are VoIP-based carrier services offered by an Internet Telephony Service Provider (ITSP) that uses the SIP protocol to set up communications between the PSTN network and inbound, outbound and/or blended calls by Five9 Agents. SIP trunks support all domestic, International, and toll-free services.

Important

To ensure that your business is not affected during data center migrations, be sure to configure a redundant data center regardless of the data center that you use. For example, if your primary data center is ATL (Atlanta), your alternate data center is SCL (Santa Clara).

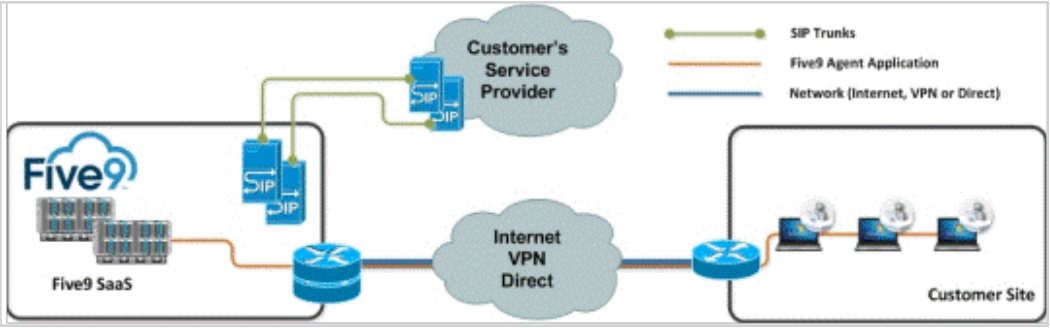
Private SIP Trunks Provided by Five9 ITSP Providers

This service originates in the Five9 data center and is connected to the PSTN network. You do not need to configure anything.



SIP Trunks Provided by Your ITSP Provider

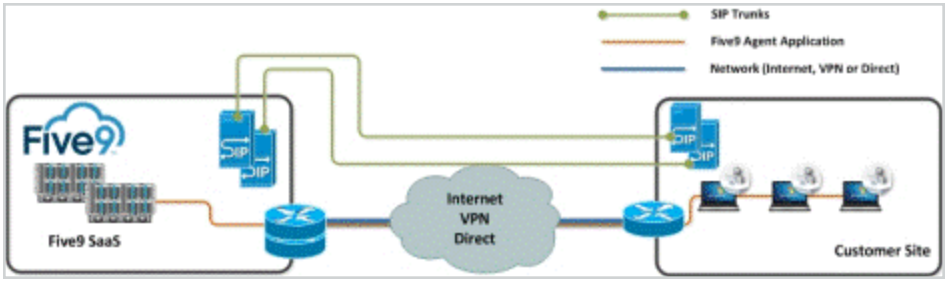
Your ITSP is connected to the Five9 SBCs in the Five9 data centers. To successfully configure, test, and turn up the SIP trunk, you must complete and return the installation checklist to Five9.



Private SIP Trunks for Five9 Gateway to Customer Gateway

If your enterprise already has or is considering a SIP Infrastructure, such as a SBC, proxy server, or SIP server, you may also select the gateway-to-gateway option. New SIP trunks are installed during the Five9 setup.

A gateway, such as AVAYA, CISCO, or Asterisk, enables you to connect to Five9 with SIP trunks across the Internet and/or through a VPN or Direct Connect Option.



Agent and Supervisor Applications

Web-Based Application Requirements

These requirements are specific to Five9 Agent Desktop Plus and Supervisor Plus, which are browser based.

If users have additional applications, be sure that each computer has sufficient hardware, a faster processor, and additional RAM to support all applications in addition to the Five9 applications.

To communicate with Five9, Agent Desktop Plus uses standard security protocols HTTPS and Secure WebSocket (WSS), which is required for proxy servers. See Supported TLS Protocols for details.

Workstations

Hardware

Windows Platforms

Component	Minimum Version or Value	Recommended
Processor	Intel Core i5-4440, CPU 2.10 GHz	Intel Core i7-4770, CPU 3.40 GHZ

Component	Minimum Version or Value	Recommended
	With Secure RTP, minimum requirements increase to Intel Pentium IV 2.66 GHZ or greater.	
Memory	8 GB	16 GB
Screen Resolution	1024 x 768	1024 x 768

Apple Mac Platforms

Component	Minimum Version or Value	Recommended
Processor	• Intel Core i5, 1.7 GHz • Apple M1	• Intel Core i7, 2.3 GHz • Apple M1
Memory	8 GB	16 GB

Chromebooks

Chromebooks are supported for WebRTC only. The Five9 Softphone plug-in cannot be installed on these products.

Component	Minimum Version or Value
Processor	Intel Core i5
Memory	8 GB

Operating Systems

Operating System	Version Supported
Windows 32- and 64-Bit	• Windows 8.1, 8.1 Professional • Windows 10, Professional, and Anniversary Update See notes about specific Windows issues.
Apple Mac	• Version 10.14 Mojave • Version 10.15 Catalina • Version 11.2.3 Big Sur
Chrome	• Versions 89.0.4389.130, 90.0.4430.215

Note

Specific Windows issues:

- Windows Media Player is not installed by default so the required MP3 codecs are absent. As a result, sound alerts and voice mail recordings cannot be played in Internet Explorer and Firefox. To resolve this issue, install the appropriate update for your platform:
  - Windows 8 N and KN
  - Windows 8.1 N and KN
  - Windows 10 N and KN
- Workstation User Access Privileges

  User Access Control (UAC) can remain enabled during installation. VCC users must, at a minimum, be standard users on their Windows workstation.
  - Windows 8 and 8.1
  - Windows 10 and 10 Pro

Web Browsers

Windows Platforms

Browser	Version
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 makes every effort to test and support the most recent version. Five9 supports 32- and 64-bit versions of the Chrome browser.
Firefox	Most recent three stable versions. Five9 supports 32- and 64-bit versions of the Firefox browser. [1]
Microsoft Edge	Most recent three stable versions. Five9 supports Microsoft Edge based on Chromium. Microsoft Edge is supported on Windows 10 Professional 64-bit. For information on downloading and installing Edge based on Chromium, see the *Microsoft Edge documentation*. **Important:** The Five9 Softphone adapter is not supported on previous versions of Edge.
Internet Explorer	Version 11. **Important**: If your customers use version 10 or lower, they do not

Browser	Version
	see preview and proactive chat, email, and survey console offers. Instead they see a message recommending that they upgrade to version 11. In that case, recommend that they enable local storage: Tools > Internet Options > Advanced > Security > Enable DOM storage.
[1] Five9 does not recommend using Firefox for WebRTC when multiple tabs are used.	

Apple Mac Platforms

Mac OS X is 64-bit only.

Browser	Version
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 makes every effort to test and support the most recent version.
Firefox	Most recent three stable versions.
Safari	Versions 12, 13, and 14 are not supported on current versions of Mac OS. [1]
[1] Versions 10 and 11 were supported on older versions of Mac OS.	

Workstation Requirements for Five9 Video Engagement

Hardware

Windows Requirements

Component	Minimum Version or Value	Recommended Version or Value
Processor	Intel Core i5-4440, CPU 2.10 GHZ	Intel Core i7-4770, CPU 3.40 GHz
Memory	8 GB	16 GB
Screen Resolution	1024 x 768	1024 x 768

Apple Mac Requirements

Component	Minimum Version or Value	Recommended Version or Value
Processor	• Intel Core i5, CPU 1.7 GHZ • Apple M1	• Intel Core i7, CPU 2.3 GHz • Apple M1
Memory	8 GB	16 GB

Operating Systems

Operating System	Version Supported
Windows 32- and 64-Bit	• Windows 8.1 • Windows 8.1 Professional • Windows 10, Professional, and Anniversary Update
Apple Mac	• Version 10.14 Mojave • Version 10.15 Catalina • Version 11.2.3 Big Sur

Web Browsers

Note

For Five9 Video Engagement, agents must install the SightCall plugin and the browser extension. For more information, see the SightCall documentation.

Windows Platforms

Browser	Version Supported
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 supports 32- and 64-bit versions of the Chrome browser.
Firefox	Most recent three stable versions. Five9 supports 32- and 64-bit versions of the Firefox browser.
Microsoft Edge	Most recent three stable versions. Five9 supports Microsoft Edge based on Chromium. Microsoft Edge is supported on Windows 10 Professional 64-bit.
Internet Explorer	Version 11, 64-bit version.

Apple Mac Platforms

Browser	Version Supported
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 supports 32- and 64-bit versions of the Chrome browser.
FireFox	Most recent three stable versions. Five9 supports 32- and 64-bit versions of the Firefox browser.
Safari	Versions 12, 13, and 14 are not supported on the current versions of Mac OS. [1]

[1] Versions 10 and 11 were supported on older versions of Mac OS.

Mobile Devices

To use Five9 Video Engagement on mobile devices, agents must install the SightCall app. A free app is provided in the app store by SightCall for iOS (version 8+) and Android (version 4.0.3+). For information on installing the SightCall app on mobile devices, see SightCall documentation.

Video Cameras

Agent Side. These cameras have been tested and are supported for Five9 Video Engagement with your Five9 interface:

- Canyon CNE-CWC3 FullHD
- Creative Live! Cam Chat HD
- Defender G-lens 2597 HD
- Genius FaceCam 1000X V2
- Logitech HD WebCam B525
- Logitech HD WebCam B910
- Logitech HD WebCam C270
- Logitech HD WebCam C310
- Logitech HD WebCam C525
- Microsoft LifeCam Cinema for Business
- Microsoft Retail LifeCam HD-3000
- Ritmix RVC-051M
- SVEN IC-950 HD
- Trust Trino HD video

Customer Side. These cameras have been tested and are supported by Five9 Video Engagement for use by customers, or contacts, during the video session:

iPad	• iPad Air • iPad 4	• iPad mini2 • iPad 2 with Retina display

	• iPad mini	
Mobile devices	• iPhone 4 • iPhone 4S • iPhone 5 • iPhone 5C • iPhone 5S	• Samsung Galaxy Note 10.1 • Samsung Galaxy Note 3 • Samsung Galaxy S4 • Google NEXUS7C ASUS • Nokia Lumia 520 • Microsoft Surface Pro
Mac OS X devices	• iMac 21.5” • MacBook Air 13” • MacBook Pro	• MacBook Air 11” • MacBook Retina 12”

Five9 Agent Assist Requirements

Agent Assist requires access to these URLs.

URL	Description
five9.net	Access to Five9 Intelligent Cloud Contact Center infrastructure and services.
launchdarkly.com	Access to feature management and continuous delivery. The public IP list for LaunchDarkly is available at: https://app.launchdarkly.com/api/v2/public-ip-list
googleapis.com gstatic.com	Access to open-source CSS and fonts.
cloud.google.com	Access to Google Cloud.
heapanalytics.com	Access to analytics of application usage.
pndsn.com	Access to messaging API (by PubNub) for client-side communication.

For Agent Assist bandwidth requirements, see Five9 Bandwidth Requirements.

Unified Communications (UC) Adapters for Skype for Business

If you choose to use Skype with Agent Desktop Plus, the Skype Web SDK is automatically downloaded to the agent's application. Therefore, ensure that agents have access to the internet or at least to the Microsoft CDN site to connect to a Lync 2013 or Skype for Business 2015 server. Agents who use the PSTN softphone connection also need a license for Lync 2011 or Lync 2013 client, which is the voice endpoint.

Virtual Desktop Infrastructure Requirements

Your agents can access Five9 Plus applications from a virtual desktop without compromising audio quality when using the softphone mode. You can use a virtual desktop with all Five9 Plus agent applications.

You may use a virtual desktop with these phone connections and channels:

- Phone connections: Five9 Softphone, PSTN, and gateway
- Channels: email, chat, and social

Gateway connections are supported with either a direct SIP station or a registered gateway SIP station with an external IP address.

Virtualization solutions with Windows Terminal Services are not officially supported by Five9. Five9 does not specify requirements or support for the virtualization server installation. For requirements and support information, contact your vendor.

The Five9 VCC Supervisor and Administrator applications are not supported with the virtual desktop.

Hardware

You may use thin or thick clients. Five9 has tested these Windows thin clients:

- Dell Wyse C9OLE7 Thin Client
- Dell Wyse Z9OD7 Thin Client

In Dell Wyse terminals, ensure that Dell Wyse File-Based Filter control (FBWF) is disabled. Too many folders in the path prevent the agent application from running.

Operating Systems

32-bit and 64-bit versions are supported in all cases.

Agent workstation thin clients:

- Windows 8 Embedded
- Windows 10

Agent workstation thick clients:

- Windows 8 and Professional
- Windows 8.1 and Professional
- Windows 10

Virtual Desktop Infrastructure

Five9 supports these platforms.

Citrix Platforms

Five9 supports these platforms:

- Citrix XenApp Server ® version 6.5+
- Citrix XenDesktop ® version 6.0+
- Citrix Virtual Apps and Desktops all versions

Important

If you use version 7.13 and newer, you must disable HDX Adaptive Protocol so ensure that the softphone is connected correctly. For more information, see How to Configure HDX Enlightened Data Transport Protocol.

This table describes the Citrix XenApp Server configuration specific to Five9. The configuration of each version may vary. Since version 7.17, Citrix XenApp Server is compatible with Firefox and Chrome 64-bit and 32-bit browsers.

Citrix Component	Version or Value
Windows Server 2008 R2, 2012 to 2016	Service Pack 1
Recommended Microsoft Patches	2465772, 2538047, 2619880, 2647582, 2769791, and all available through Windows Update (2013-10-24)
Registry	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook`: Verify that `ExcludedImageNames` does not contain firefox.exe or chrome.exe.
Remote Desktop Session Host Configuration	Audio playback, audio recording: Allowed Session IP Virtualization: Enabled
XenApp Server Policies	Computer: • Virtual IP loopback support: Enabled • Virtual IP virtual loopback programs list: add java.exe, javaw.exe, javaws.exe, Five9SoftphoneService.exe, firefox.exe, and chrome.exe.
	User: • Client audio redirection: Allowed • Client microphone redirection: Allowed
Citrix Receiver	Microphones/Webcams (Connection Center): Full Access

VMware Platforms

Five9 supports version 6.0 and higher and Horizon Client version 4.3.

Java-Based Application Requirements

These requirements apply to the Five9 Agent Desktop and Supervisor applications. Agents who run additional software applications require additional RAM and a faster processor. Ensure that each desktop has sufficient hardware to support all applications, including the Five9 application. Supervisors running reporting applications require additional memory. See Workstation Requirements for Spreadsheet Dashboards.

Note

Five9 does not recommend using MacOS Big Sur or Safari 14 for Java-based applications.

Hardware

Windows Platforms

Component	Version or Value	Recommended Version or Value
Processor	Intel Pentium IV 1500MHZ or greater, or equivalent (based on published benchmark results)	Intel Pentium IV 2400 MHZ or greater, or equivalent (based on published benchmark results)
Memory	1.5 GB or higher with Windows 8	2.0 GB or greater
Screen Resolution	1024 x 768 or higher	1024 x 768 or higher

Apple Mac Platforms

The Apple Mac platform is supported for the Five9 VCC Administrator, Desktop Agent, Supervisor, and Five9 stateless adapters for Salesforce, Agent Desktop Toolkit, NetSuite, Oracle, and Velocify.

Important

Versions 3 and 4 of the Five9 ***CTI*** Adapter for Salesforce are not supported on Mac OS X platform. The Five9 ***Open CTI*** Adapter for Salesforce is supported on Mac OS X releases.

Component	Minimum Version or Value	Recommended Version or Value
Processor	Intel Core i5, 1.7 GHz Intel Core i7, 2.3 GHz	Intel Core i5, 1.7 GHz Intel Core i7, 2.3 GHz
Memory	2GB of RAM	2GB of RAM

Java Runtime

Warning

Due to changes to the Oracle Java SE Support Roadmap, you are required to purchase a Java SE Subscription to receive future updates of Oracle Java SE products.

The Five9 Administrator, Supervisor, and Agent applications will continue to work with Oracle Java SE. For the latest Java SE versions supported by Five9, refer to the Five9 Technical Requirements Reference Guide. To purchase a Java SE subscription, visit Oracle Java SE Subscriptions.

Because the Five9 web-based applications do not require Java SE, Five9 strongly recommends that you migrate to the Five9 Plus applications. For more information about the migration, contact your Five9 representative.

Component	Version
Java Runtime Environment	8.0 updates 281, 291, and 301. For Windows systems, the 32-bit version is required to use the softphone and the script and browser tabs in the Desktop Agent application.

Operating Systems

Windows and Mac (32- and 64-Bit)

Operating System	Version Supported
Windows 32- and 64-Bit	• Windows 8, 8 Professional • Windows 8.1, 8.1 Professional • Windows 10, 10 Professional
Apple Mac	• Versions 10.7 Lion to 10.13 High Sierra included

Five9 Agent or Supervisor Workstation User Access Control

Operating System	Version and Notes
Windows 8 and 8.1 Windows 10 and 10 Pro	User Access Control (UAC) can remain enabled during installation. At a minimum, VCC users must have standard access to their Windows workstation.

Web Browsers

Five9 supports 32- and 64-bit versions of the Chrome browser.

Windows Platforms (32-bit version only)

Browser	Version
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 makes every effort to test and support the most recent version.
Firefox	Most recent three stable versions. Firefox is supported on Windows 32-bit and 64-bit operating systems.
Internet Explorer	Version 11

Apple Mac Platforms

Browser	Version
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 makes every effort to test and support the most recent version.
Firefox	Most recent three stable versions. Firefox is supported on Windows 32-bit and 64-bit operating systems.
Safari	• Versions 10 and 11. • Versions 12, 13, and 14 are not supported.

Five9 Supervisor

In addition to requirements listed in above, supervisors who use additional software applications may require more RAM and a faster processor. Ensure that each workstation has sufficient hardware to support all running applications.

Apple iPad

This section applies to the iPad Supervisor application. It does not apply to Supervisor Plus and the Java Supervisor client.

- System Requirements

Model	Operating System
iPad Air	iOS 12.0
iPad mini 2 (Retina)	iOS 12.0
iPad 4	iOS 10.3.3 Latest for the device
iPad mini	iOS 9.3.5 Latest for the device
iPad 3	iOS 9.3.5 Latest for the device

- Codecs: The primary codecs are G711U and G711A. You may also use GSM or ILBC, but these have not been tested.
- Browsers: Safari and Chrome
- Headsets: Supervisors may use any headset compatible with iPad and any Advanced Audio Distribution Profile-compatible (A2DP) Bluetooth device that is certified by Apple for use with iPad devices.

Workstation Requirements for Spreadsheet Dashboards

Component	Version
Processor	Intel Pentium IV 2400 MHZ or greater, or equivalent
Memory	3.0 GB or greater
Application	Microsoft Office 2003 or later

Headset for Agents and Supervisors

Five9 recommends USB-connected headsets with noise canceling features. Analog headsets are not supported. Wireless LAN technology often results in degradation of call voice quality, causes a delay between the audio played and heard, and can present other audio issues. Because these issues contribute to a lower-quality customer experience, Five9 does not recommend wireless headsets when more than 10 agents are active at the same time. For suggested devices, see Five9 Recommended Headsets.

Application Notes

Web Page Security and Visual IVR Scripts

VCC administrators can apply web page security to Visual IVR scripts to prevent these scripts from being embedded in a web page X-frame where the user can be hijacked to another page. Not all browsers support X-Frame in the same way. This table lists the browsers and versions that support X-Frame-Options HTTP header that is used with the Five9 Web Page Security feature.

To test any other browser version, use this page: http://erlend.oftedal.no/blog/tools/xframeoptions/. For more information, refer to the Interactive Voice Response (IVR) Administrator's Guide. Five9 Visual IVR does not work if Internet Explorer is set to Compatibility View.

Browser	Version Supported	Version Partially Supported
Chrome		46, 47, 48, 54, 56, 67 52, 56 (Android phones)
Firefox	18 – 79	17
Internet Explorer	11 Windows phone	
Safari	8, 9	10.0.1
Opera		26
**ALLOW_FROM value not supported.*		

Dashboards

The browser must support Secure WebSocket (WSS) and SVG. Dashboards do not work if the browser is set to Compatibility View.

Agent Desktop Plus with Digital Engagement

Some antivirus software, such as Avast! Antivirus, might interfere with the ability to use the chat, social, or email because the software prevents text media from loading.

Integrated Administration Console

Browser requirements for integrated administration console:

Browser	Version
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 makes every effort to test and support the most recent version.

Five9 Agent Integrations

Requirements for Web-Based Adapters

These requirements apply to Five9 Plus adapters:

- Five9 Plus Adapter for Agent Desktop Toolkit
- Five9 Plus Adapter for Salesforce
- Five9 Plus Adapter for Oracle
- Five9 Plus Adapter for NetSuite
- Five9 Plus Adapter for Microsoft Dynamics 365
- Five9 Plus Adapter for Zendesk
- Five9 Plus Adapter for ServiceNow

Ensure that each desktop has sufficient hardware to support all applications that are running on the desktop alongside the Five9 application. Agents running additional software applications might require additional RAM and a faster processor.

The Five9 Plus adapters use standard security protocols HTTPS and Secure WebSocket connections to communicate with the Five9 environment. If you plan to use proxy servers, the servers must support Secure WebSocket. See Supported TLS Protocols for details.

Workstation Requirements

Hardware

Windows Platforms

Component	Minimum Version or Value	Recommended Version or Value
Processor	Intel Pentium IV 1500MHZ or greater, or equivalent (based on published benchmark results)	Intel Pentium IV 2400 MHZ or greater, or equivalent (based on published benchmark results)
Memory	1.5 GB or higher with Windows 8	2.0 GB or greater
Screen Resolution	1024 x 768 or higher	1024x768 or higher

Note

If you enable Secure RTP, the minimum workstation requirement is Intel Pentium IV 2.66 GHZ or greater and 1.5 GB memory.

Apple Mac Platforms

Component	Minimum Version or Value
Processor	• Intel Core i5, 1.7 GHz • Intel Core i7, 2.3 GHz • Apple M1
Memory	8 GB of RAM

Operating Systems

Operating System	Version Supported
Windows 32- and 64-Bit	• Windows 8, 8 Professional • Windows 8.1, 8.1 Professional • Windows 10, Professional
Apple Mac	• Version 10.14 Mojave • Version 10.15 Catalina • Version 11.2.3 Big Sur

Web Browsers

For information about the browser configuration specific to your Plus adapter, see the guides for your integration.

Browser	Version Supported	Platforms
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 makes every effort to test and support the most recent version. Five9 supports 32- and 64-bit versions of the Chrome browser.	Windows and Mac
Firefox	Most recent three stable versions. Five9 supports 32- and 64-bit versions of the Firefox browser.	Windows and Mac
Microsoft Edge	Most recent three stable versions. Five9 supports Microsoft Edge based on Chromium. Microsoft Edge is supported on Windows 10 Professional 64-bit. For information on downloading and installing Edge based on Chromium, see the *Microsoft Edge documentation* **Important:** The Five9 Softphone adapter is not supported on previous versions of Edge.	Windows
Internet Explorer	Version 11. Version 10 is not supported. **Important:** If you use multiple applications and multiple browser tabs, Five9 does not recommend that you use the softphone with Internet Explorer. • Salesforce Sales Cloud: Due to potential performance issues, Five9 recommends that agents working with multiple tabs do not use Internet Explorer 11. • Salesforce Lightning: 32- and 64-bit versions. • Plus Adapter for Oracle Service Cloud: Requires Internet Explorer. However, because this version cannot play WAV files, agents may not hear notifications for inbound calls if they disable **Auto-Answer Inbound/Autodial Calls** in their softphone settings.	Windows
Safari	• Versions 12, 13, and 14 are not supported on current versions of Mac OS. [1]	Mac

[1] Versions 10 and 11 were supported on older versions of Mac OS.

Application Requirements

Plus Adapter for Agent Desktop Toolkit

If you use Internet Explorer 11, ensure that TLS 1.2 is the default for the browser and the computer and that .NET Framework version 4.5 or higher is installed.

Plus Adapter for Salesforce

The current Managed Package version is 2.46. The supported SAML version is 2.0.

Five9 supports the Salesforce Lightning CTI mode, Sales Cloud, and Service Cloud with the Professional, Enterprise, Unlimited, and Performance editions. The Plus Adapter for Salesforce Lightning Experience is supported, except for these operating system and Internet Explorer combinations:

- Windows 8.1 Professional 64 bit with Internet Explorer 11.0.9600.16384
- Windows 10 Professional 32 bit with Internet Explorer 11.0.10240.17394
- Windows 10 Professional 64 bit with Internet Explorer 11.0.10240.17394
- Windows 10 Enterprise 64 bit Internet Explorer 11.0.10240.17394

Plus Adapter for Oracle Service Cloud

To use the chat feature, the Five9 Plus Adapter requires at least Oracle Service Cloud 2014 server.

Plus Adapter for NetSuite

If you use Internet Explorer 11, ensure that TLS 1.2 is the default for the browser and the computer and that .NET Framework version 4.5 or higher is installed.

Plus Adapter for Microsoft Dynamics 365

The adapter requires at least these versions:

- Microsoft Dynamics 365 Online version 9.0.
- Microsoft Dynamics 365 (On-Premises) version 2013 or higher. Internet Explorer 11 is not supported.

Microsoft Dynamics 365 Channel Integration Framework enables developers to build third-party communication applications to integrate voice and Digital Engagement. Five9 provides limited support for Microsoft Dynamics 365 Channel Integration Framework. For more information, contact your Five9 representative.

In Mac platforms, users of Microsoft Dynamics 365 are limited to the Safari browser.

Plus Adapter for Zendesk

The adapter requires at least Zendesk Support and Zendesk Talk - Partner Edition (see zendesk.com/talk/pricing). To play recordings, the Zendesk application requires Adobe Flash Player.

Plus Adapter for ServiceNow

The adapter supports the Classic and Agent workspaces and is compatible with the Orlando, London, Madrid, and New York versions.

Requirements for Java-Based Adapters

Workstation Requirements

Hardware

Component	Version
Memory	Add 512 MB to agent desktop requirements.

Operating Systems

Operating System	Version Supported
Windows 32- and 64-Bit	• Windows 8, 8 Professional • Windows 8.1, 8.1 Professional • Windows 10, Professional
Apple Mac	• Version 10.14 Mojave • Version 10.15 Catalina • Version 11.2.3 Big Sur

Java Requirements

Component	Version
Java Runtime Environment (JRE)	8.0 updates 281, 291, and 301. The 32-bit version is required for softphone use. The adapters for NetSuite and Velocify do not work with version 251.

Web Browsers

The softphone requires a 32-bit version.

Browser	Version Supported	Platforms
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 makes every effort to test and support the most recent version. Except for Salesforce Open CTI, Chrome cannot be used on Mac platforms. Five9 supports 32- and 64-bit versions of the Chrome browser.	Windows and Mac
Firefox	Most recent three stable versions. The adapters for NetSuite and Velocify do not support these versions. Five9 supports 32- and 64-bit versions of the Firefox browser. **Important:** Note for Agent Desktop Toolkit, NetSuite, and Velocify: If you use the 64-bit version, you cannot automatically install the extensions. To install them manually, follow these steps: **1** Download and install the adapter. The extension file is placed in the user's file system. **2** In Firefox, either click the menu button and choose **Add-ons**, or select **Tools > Add-ons**. **3** On the left, click **Extensions**. **4** At the top right, click the cog icon, and select **Install Add-on From File**. **5** Locate and open the extension file: `c:\Users\<USERNAME>\AppData\Roaming\Five9 \Integrations\Firefox Extensions\f9adt.xpi`	Windows and Mac
Internet Explorer	Version 11	Windows

Browser	Version Supported	Platforms
	Important: If you use multiple applications and multiple browser tabs, Five9 does not recommend that you use the softphone with Internet Explorer. This note applies to all CRM integrations.	
Safari	• Versions 12, 13, and 14 are not supported on current versions of Mac OS. [1]	Mac
[1] Versions 10 and 11 were supported on older versions of Mac OS.		

Application Requirements

Five9 Agent Desktop Toolkit

This adapter supports only the voice channel. It cannot be used for Digital Engagement.

Five9 Open CTI Adapter for Salesforce

These Salesforce versions are supported:

Salesforce Product	Version Supported
Salesforce	Unlimited, Enterprise, and Professional Editions
Service Cloud Console	Supported when used in a supported edition
Partner Edition	Not supported

Salesforce.com determines the web browsers and their versions supported for the Salesforce development toolkit. Browsers are 32-bit versions only.

Five9 Adapter for NetSuite

Five9 supports the current and previous versions of NetSuite CRM+.

Five9 Adapter for Oracle Service Cloud

The adapter requires Microsoft .NET Framework, version 4.0.

Five9 Adapter for Velocify

Five9 supports the current and previous versions of Velocify Small Business and Enterprise. Your version of Velocify must support XML Post capabilities.

Five9 Cloud API Web Services (Custom Integration)

The Five9 Cloud API web services enable you to create custom integrations. APIs contain technical limits designed to prevent excessive use that may degrade overall performance of the API services. Refer to the API documentation for the current limits for each API.

Verint Systems Requirements

Verint Systems® is a browser-based application that provides agent analytics and performance evaluation.

Workstation Requirements

These requirements assume the Five9 Virtual Contact Center and Verint Systems products are the only applications running in the agent's workstation. Agents who use additional software may require additional RAM and a faster processor. Sufficient hardware to support all agent applications is at the discretion of the administrator. Some features may require additional workstation components.

To allow your agents to create and leave conferences that contain an unlimited number of participants, request from your Five9 representative that your domain be enabled. As part of that process, you will be required to acknowledge that you will be responsible for toll charges if your agents set up external non-business-related conferences.

Hardware Requirements

Component	Requirement
Processor	Minimum: 2 GHz; recommended: 3.2 GHz
Memory	Minimum: 2.0 GB; recommended 4.0 GB.

Component	Requirement
Disk Space	For desktop and process analytics: 10 MB for the client installation files and 100 MB to ensure that processes run when there is no network access.
Monitor	Minimum resolution: 1280 x 800 Recommended resolution: 1280 x 1024 or higher
Video Card	Video card with 32MB RAM minimum.
Network	10-100 Mbps 10-BaseT LAN Card.

Third-Party Software Required for Agent Stations

The Five9 and Verint Systems® CTI integration supports a secure instance of Verint Systems 15.2 Workforce Optimization solution.

Important

A VPN or MPLS application may be required for Verint Systems.

This table lists the minimum third-party software requirements for the desktop application installed in each agent's computer.

Important

Install the desktop resources package before installing any other desktop application.

You must manually enable the .NET Framework 3.5 SP1 for desktop applications that run on Windows 8.x operating systems.

Desktop Application	Required Third-Party Software
Desktop Resources	Microsoft Windows Installer 5.0 or later.
Desktop and Process Analytics (DPA) Client	• Microsoft .NET Framework 4.6.2 or 4.7.x. • Microsoft Windows Installer 5.0. • Microsoft Message Queue (MSMQ) is required for all versions of the DPA Client. The MSMQ Server and MSMQ Server core features are required. System restart is required before installing the DPA client. • Microsoft Visual C++ 2015 Redistributable. On a 64-bit system,

Desktop Application	Required Third-Party Software
	both 32-bit and 64-bit redistributables must be installed.
DPA Validator	• Microsoft .NET Framework 4.6.2 and higher versions supported by Microsoft on the Windows operating system. • Microsoft Visual C++ 2015 Redistributable requires both 32-bit and 64-bit redistributables.
DPA Process Discovery	• Microsoft .NET Framework 4.6.2 or 4.7.x. • Microsoft Visio: Version 2010, 2013, or 2016. • Visual Studio Tools for Office Runtime: Version 4.0.
Form Designer & Form Designer (standalone)	• Microsoft Windows Installer 5.0 or later. • Microsoft .NET Framework 4.6.2, or 4.7.x. • Microsoft Visual C++ 2015 Runtime 32-bit or later with applicable service packs and updates installed.
Logger	• Microsoft Windows Installer 5.0 or later. • Microsoft .NET Framework 4.6.2 or 4.7.x. • Microsoft Visual C++ 2015 Redistributable 32-bit or later with applicable service packs and updates installed.
Plugin Player	Internet Explorer requirements: • Microsoft Windows Installer 5.0 or later • Microsoft DirectX 9C or later • MSXML 6 32-bit • Microsoft .NET Framework 4.6.2or 4.7.x • Microsoft Visual C++ 2015 Redistributable 32-bit or later with applicable service packs and updates installed. There are no additional requirements for Google Chrome.
Screen Capture Module	• Microsoft Windows Installer 2.0 or later. • Microsoft Visual C++ 2019 Redistributable 32-bit. • Microsoft .NET Framework 4.6.2or 4.7.x
Strategic Planner	• Microsoft Windows Installer 5.0 or later • Java Run-time Environment (JRE) 8.0 (32-bit) including all approved minor version releases • Visual C++ Redistributable for Visual Studio Update 4

Third-Party Software Required for Browsing

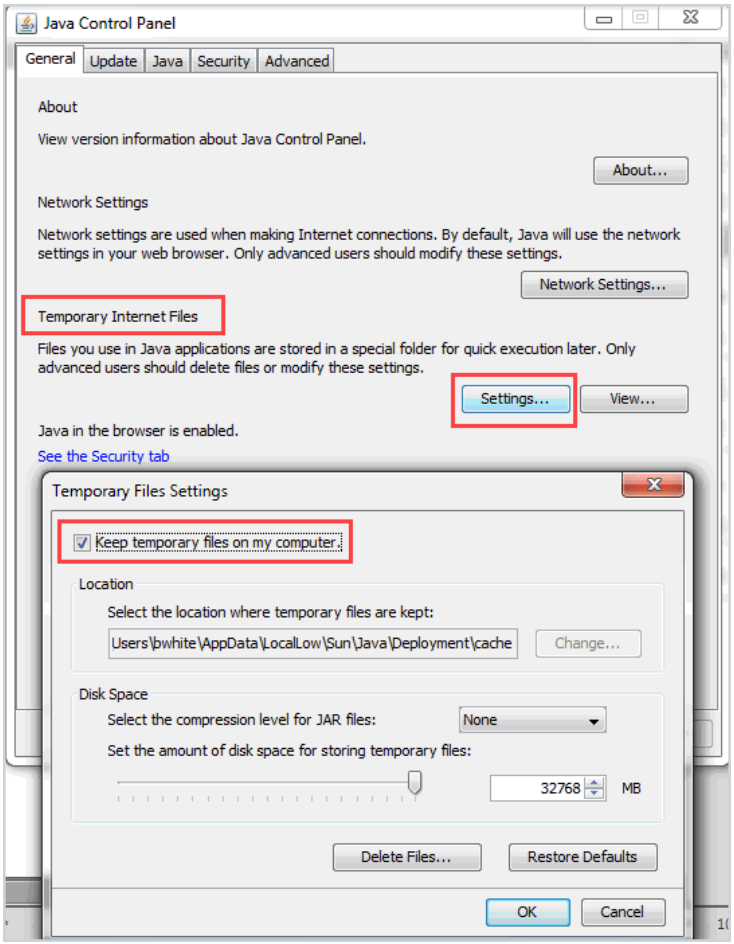
This table lists the software required to enable users (typically administrator or supervisor) to browse web-based applications:

Software	Web-Based Application
Adobe Reader, version 11 or higher	Required for printing reports.
Java Runtime Environment (JRE) 8.0 (32-bit) including all approved minor version releases.	The following web desktop applications require JRE: • Strategic Planner
Windows Media Player 12	Required to play files from workstations without browsing to the Interactions Home Page.

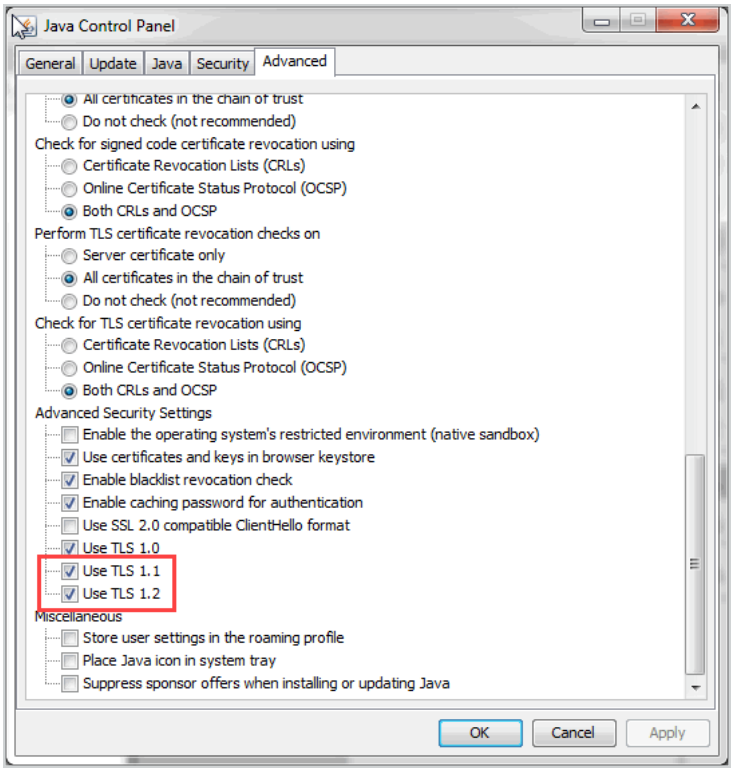
JRE Settings Requirements

Verify the following JRE settings:

- In the Java Control Panel, enable **Keep temporary files on my computer** in all client workstations. Otherwise, each time that users log in, security prompts are displayed.



- For systems using SSL with High Mode, in the Java **Control Panel > Advanced > Advanced Security Settings**, enable **Use TLS 1.1** and **Use TLS 1.2**. These are required to support WFM Pulse, Adherence, and Calendar applet pages.



Supported Operating Systems

Operating System	Version Supported
Microsoft Windows 8, 8.1 Pro, and Enterprise	64-bit
Microsoft Windows 10 Pro and Enterprise	32-bit and 64-bit

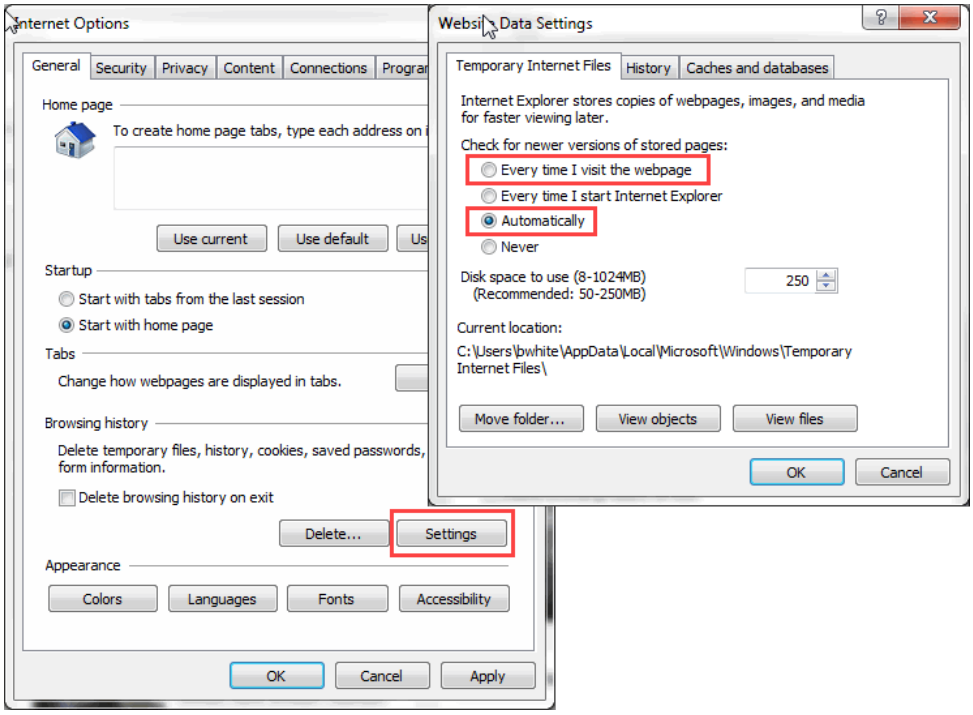
Supported Web Browsers

Internet Explorer

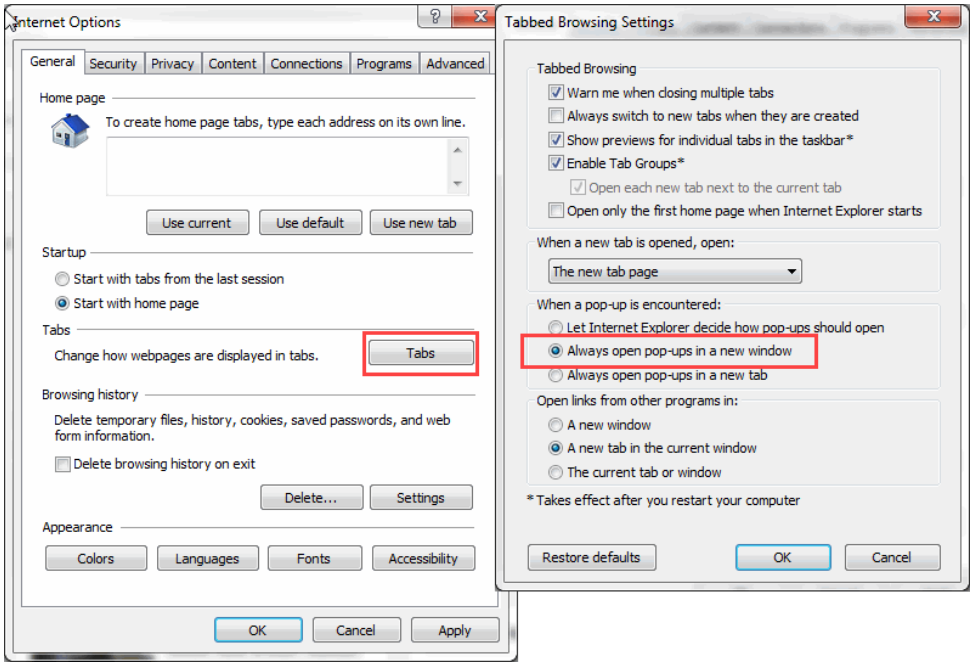
Internet Explorer version 11 is supported. To prepare your browser, complete these steps:

1 To allow dynamic updates of pages during user sessions, in **Internet Options > General**, in the general tab, click **Settings > Temporary Internet Files > Automatically** or **Every time I visit the web page >** Click **OK**.

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



2 To adjust pop-up settings, in the general tab, click **Tabs**, select **Always open pop-ups in new window**, and click **OK**.



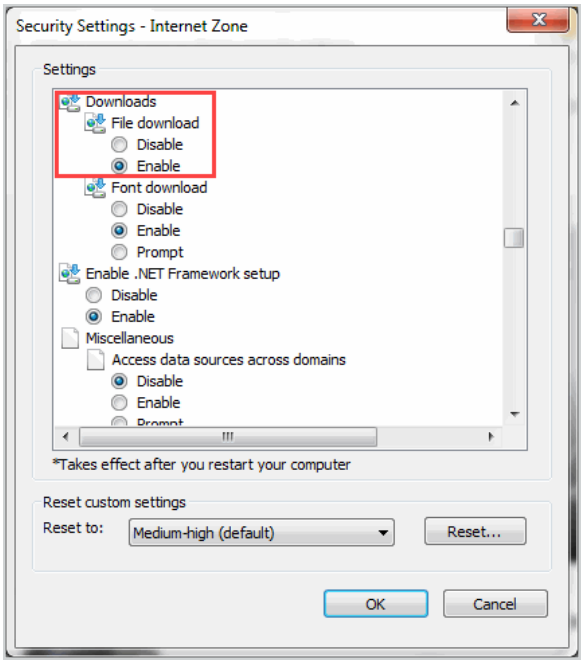
3 In the **Security** tab, set these options for the **Internet Zone**:

   a Select **Custom level > ActiveX controls and plug-ins** and set these options:

   - Binary and script behaviors: **Enable**.
   - Download signed ActiveX controls: set as **Enable** or **Prompt**.
   - Download unsigned 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**.

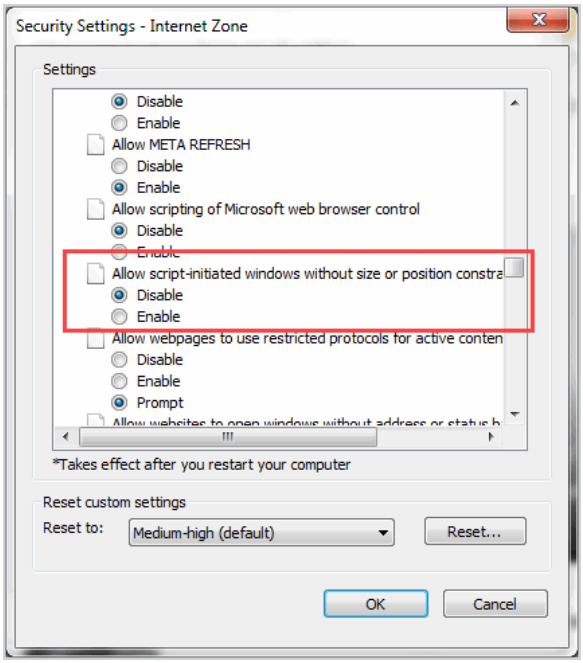
   ActiveX controls and plug-ins are required for playback, import/export manager, and to import users from your domain.

   b To enable downloading files from the portal and to enable call forwarding from the Interactions Portal, scroll to the **Downloads** section and set File download to **Enable**.



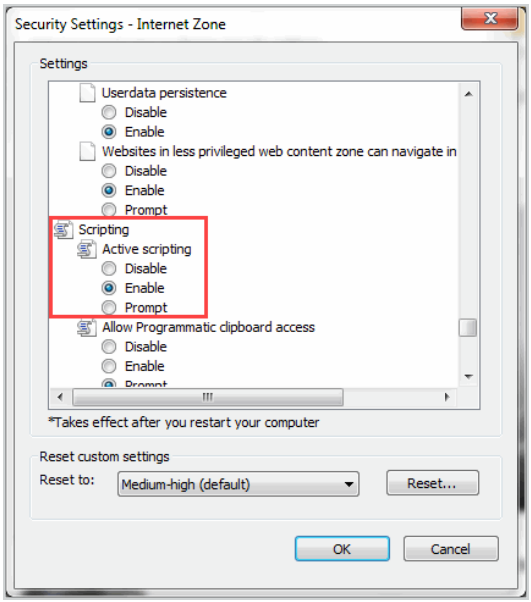
c Scroll down to the Miscellaneous section, and enable **Allow script-initiated windows without size or position constraints**.

Script-initiated windows are required for login, interaction administration applications, play screen (in a new window), System Monitor, and Recorder Manager.



d Scroll down to the **Active Scripting** section, set these options:

- Active Scripting: **Enable**



- Scripting of Java applets: **Enable** or **Prompt**.

Scripting of Java applets is required for Project Rules Manager and WFM applications.

e In the **User Authentication** section, set these options:

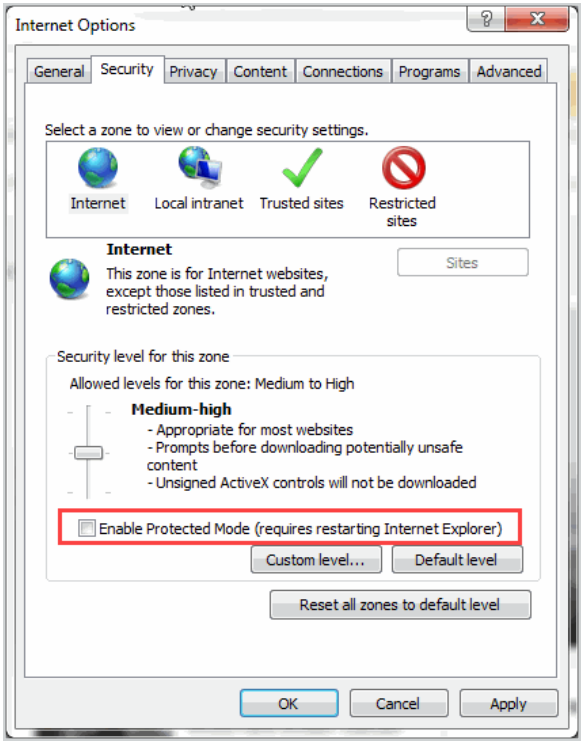
- **Automatic logon with current username and password** (internet zone)

  or

- **Automatic logon only in Intranet zone** (local intranet or trusted zones)

f Click **OK**.

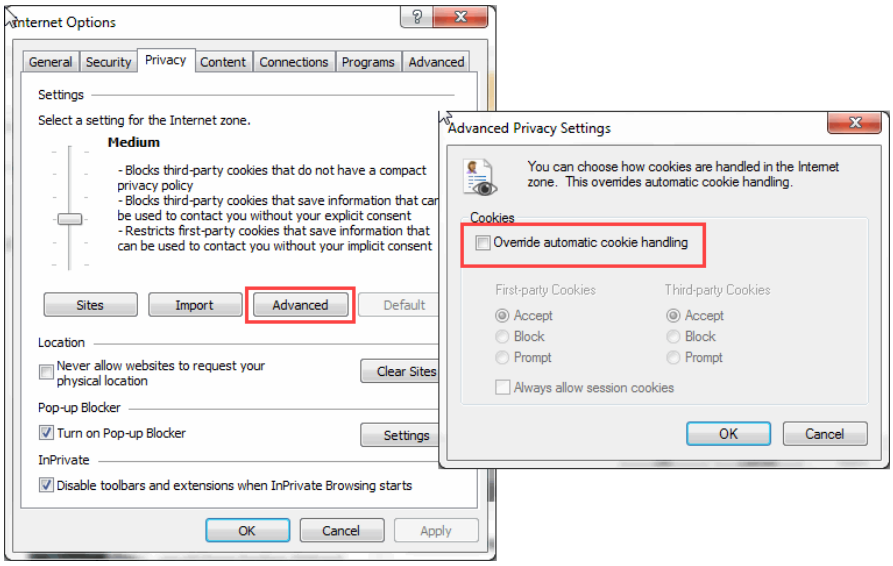
g Disable **Enable Protected Mode**.



4 In the **Privacy** tab, verify these settings:

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

b Click **Advanced,** disable **Override automatic cookie handling**, and click **OK**.



c In **Pop-up Blocker**, click **Settings**. In the field, enter the Portal URL and click **Add**.

This URL is required for the login and popup windows of QM administration applications System Monitor and RM.

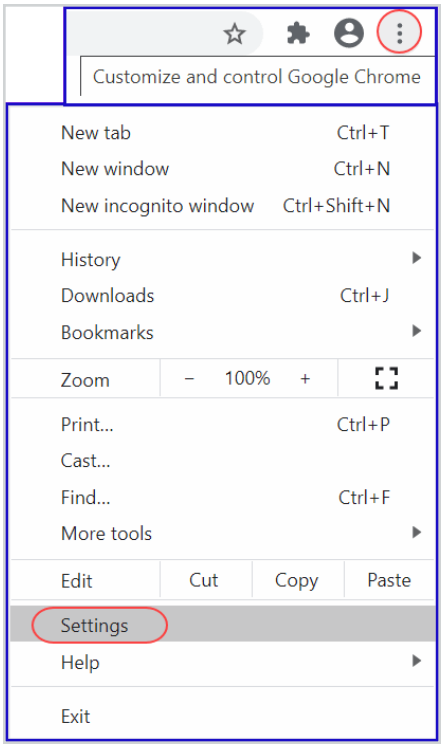
5 In the **Advanced** tab, scroll to Security and enable **Enable Integrated Windows Authentication**.

Google Chrome

Google Chrome, version 45 or higher, is supported on Windows 32-bit and 64-bit operating systems. The general Chrome settings described here apply to all desktop applications. The location of the settings shown here use Chrome version 84, the location you see may differ with Chrome version updates.

To configure your Chrome browser, follow these steps.

1 Navigate to **Settings** using the Google Chrome Customize and Control menu.



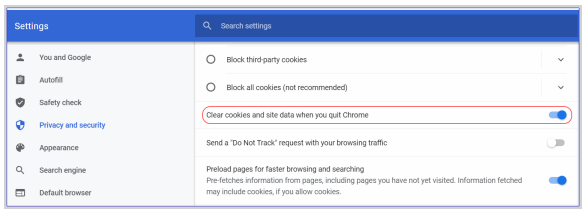
Verint uses cookies to maintain user sessions and load balance persistence.

2 Add the portal address to the list of sites allowed to use cookies.

You can determine whether to close session recording when the active window is closed, or allow session persistence, based on your business needs.

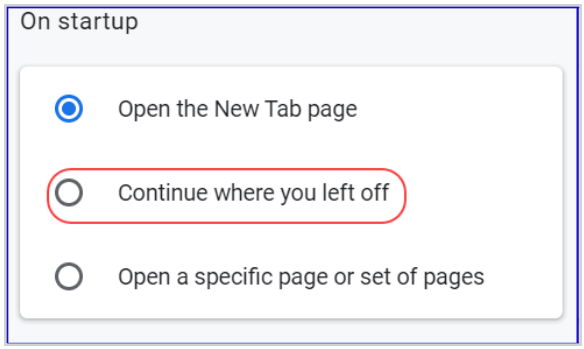
3 Define your session close options using one of the following options.

a To complete the recording session when the active window is closed, enable **Clear cookies and site data when you quit Chrome**.

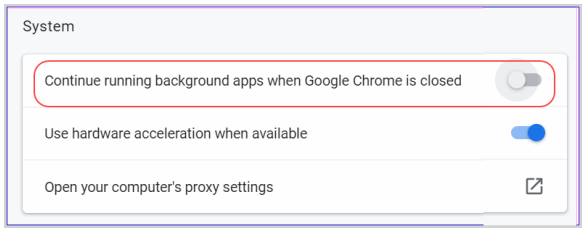


or

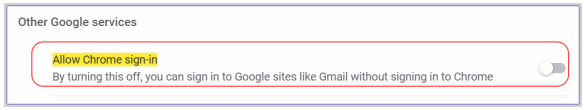
b Clear **Continue where you left off**.



c Clear **Continue running background applications when Google Chrome is closed**.

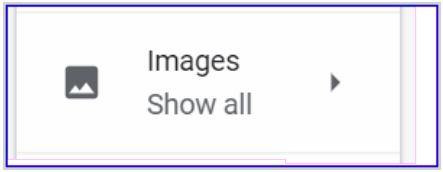


d Clear **Allow Chrome sign-in**.

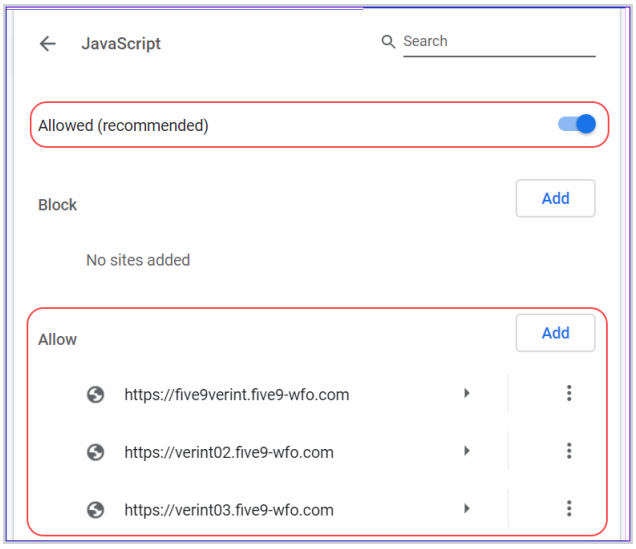


Images must be enabled to show the images and icons of the player application.

4 Enable **Show all images**.



5 To enable JavaScript, select **JavaScript Allowed**.



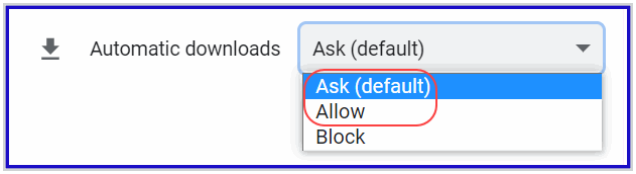
6 To add the five9-wfo portal addresses to the list of sites allowed to run JavaScript, click **Add**.

Pop-ups are required for the following pop-up windows:

- Login
- Interaction administration applications
- Play screen in a new window
- DPA portal

7 To enable pop-ups, select **Pop-ups Allowed** and add the **five9-wfo** sites to the list of sites allowed to display pop-ups.

8 To enable files being downloaded from the portal, such as DPA validator and reports, select **Ask** or **Allow** for automatic downloads.



Browser Requirements for Verint Player

Windows Media Player is the default player used when working in Microsoft Internet Explorer. Google streaming media player is used when working in Google Chrome.

Interaction playback in Chrome or Internet Explorer version 11+ using MIcrosoft Windows version 8 or newer streams playback and deoes not require installation of the Playback MSI on the user's desktop. The player uses the native browser capabilities to perform playback. When playing interactions in Internet Explorer using regular playback, desktop installation is required.

Network Requirements (LAN and WAN)

A site-to-site VPN may be required for customers who use Verint Call Recording, Verint Screen Recording, Verint Quality Management, Verint Advanced Desktop Analytics, Verint Analytics Driven Quality, and Verint Speech Analytics. A VPN connection is no longer required to access Verint Workforce Management or Verint Performance Management.

If you use Screen Recording, an additional 160kbps is required for each agent in addition to the stated bandwidth requirements. For Verint Systems QM customers using legacy screen recording, be sure to meet these requirements:

- 1:1 NAT for VPN
- Customer private connectivity for screen recording and real-time monitoring

For more information, see Five9 Network Requirements (LAN and WAN).

Firewall Requirements

These ports need to be open for Verint application features. These ports apply to US and EU environments.

Port Number	TCP/UDP	Inbound/Outbound	Server-Side Components
443	TCP	Outbound	Verint Systems Application Suite
3520-3590	TCP	Outbound	Verint DPA customers only (RIS)
4001	TCP	Inbound	Verint Systems Screen Recorder
8500-8510	UDP	Inbound	Verint Recorders
29434	TCP	Outbound	Verint Systems Cloud Screen Recorder
29522, 29436	TCP	Outbound	Verint Systems RIS servers

Calabrio Application Requirements

The Five9 and Calabrio® Product integration is a CTI integration that supports a secure instance of the Calabrio One Smart Desktop. The Calabrio One Smart Desktop captures all user data (call recording, screen recording, call metadata, and desktop application activity) in an agent's desktop.

> **Note**
> Data gathered is based on licensing and permissions enabled.

Desktop Requirements

> **Note**
> You may manage all desktop software requirements with Group Policy.

Windows Operating Systems

The following operating systems are validated for use with Calabrio One Smart Desktop.

Operating System	Restrictions
Windows 10 (32&64-bit)	None.
Windows 8.1 (32&64-bit)	Requires Update 1.

.NET Framework

Calabrio ONE Smart Desktop requires .NET framework 4.5.1 or later for Desktop Analytics features and functionality.

Web Browsers

The following web browsers may be used with the Calabrio ONE Smart Desktop:

Important

Be sure to disable pop-up blockers so that you can download files from calabriocloud.com.

Web Browser	Restrictions
Internet Explorer	Versions 10 and 11 (32 & 64-bit) Using Calabrio ONE requires that WebM Media Foundation components be installed on Supervisor desktops. This codec allows audio and video stream recording playback in Internet Explorer web browsers. This codec is required only for Internet Explorer playback.
Google Chrome	None.
Firefox	• 32-bit • Version 42 or later.

Capture Bandwidth

The following bandwidth requirements are necessary for Smart Desktop capture:

- Screen capture: 1.5 MB/min (MV4 format)
- Audio capture: 0.5 MB/min (OPUS format)

Analytics and Plug-in Extensions

Calabrio ONE Smart Desktop uses browser extensions and/or plug-ins for desktop analytics features – web application usage and work flow triggers using desktop events.

The Internet Explorer and Firefox extensions are installed with the Calabrio ONE Smart Desktop. Enabling these extensions can either be done manually or through Group Policy.

The Google Chrome extension can be manually downloaded from the Chrome store or installed through Group Policy.

Five9 recommends to manage these plug-ins and extensions through Windows Group Policy to ensure that all features dependent on the plug-ins/extensions installed are working as designed.

Antivirus Real-Time Scanning Exclusions

To ensure that all Smart Desktop features function as expected, Five9 recommends that you exclude these Calabrio directories from Antivirus real-time scans:

- For 64-bit Windows Operating Systems
  - C:\ProgramFiles(x86)\CalabrioONE\Desktop*
  - C:\ProgramFiles(x86)\CommonFiles\CalabrioONE\Desktop*
- For 32-bit Windows Operating Systems
  - C:\ProgramFiles\CalabrioONE\Desktop*
  - C:\ProgramFiles\CommonFiles\CalabrioONE\Desktop*

Firewall Requirements

Add `https://*calabriocloud.com` to your firewall list of allowed URLs.

If you use an internet proxy, it must support secure WebSocket connections for the Calabrio Smart Desktop client.

For more information about managing and updating the Calabrio ONE Smart Desktop and uploading recordings to the Calabrio cloud, refer to the Calabrio Administrator's Guide.

Studio Requirements

Five9 Studio Intelligent Virtual Agent and Interactive Voice Response services can integrate to APIs over the internet.

Public Internet Domains

This table lists the URLs to access the Studio Portal.

URL	Location	Services
https://five9.us.studioportal.io/	US, South America	Studio Portal, Studio API
https://five9.au.studioportal.io/	Australia, New Zealand, Japan, South East Asia	Studio Portal, Studio API
https://five9.ca.studioportal.io/	Canada	Studio Portal, Studio API
https://five9.uk.studioportal.io/	EU, UK, Africa	Studio Portal, Studio API

Web Service Integration IP Addresses

If you use a firewall to restrict access to specific sources, ensure that you add the following IP addresses to your IP allow list.

Note

All outbound requests from integration nodes and web services hosted internally by Five9 will use the following IP addresses. Externally hosted services sush as Google App Engine or AWS will not use the IP addresses listed.

USA Integration IPs.

Virginia (Primary Site)	Chicago (Secondary Site)
199.189.191.86	199.189.190.142
199.189.191.146 (alternate)	

Virginia PCI (Primary Site)	Chicago PCI (Secondary Site)
199.19.68.222	199.189.190.142

Australia Integration IPs.

Melbourne (Primary Site)	Sydney (Secondary Site)
202.147.140.98	202.147.130.70

Melbourne PCI (Primary Site)	Sydney PCI (Secondary Site)
202.147.129.154	202.147.130.92

UK Ireland Integration IPs.

Primary AZ	Secondary AZ
34.248.214.96	34.249.108.45
	34.250.28.125 (alternate)

Canada Integration IPs.

Primary AZ	Secondary AZ
35.182.62.129	35.183.166.219

SBC Public IP Addresses

Note

- Studio SIP signaling uses UDP port 5060; Secure SIP TCP port 5061 in beta release; Secure Call Proxy UDP port 5189; Secure SIP TCP port 5161.
- RTP Media uses UDP ports 35000 - 65000 for PCI, AWS and SNSW icare (Aus PoP) otherwise 10200 - 28000.
- Legacy trunks used UDP port 5188 for SIP signaling.

Note

DNS SRV is the preferred method to use when connecting to Five9 SIP resources.

Customers and partners wishing to allow specific IPs need to monitor the provided domains for changes to underlying IPs offered.

USA SBC IPs.

Virginia (Primary Site)	Chicago (Secondary Site)
199.189.191.98	208.71.166.115

Virginia PCI (Primary Site)	Chicago PCI (Secondary Site)
199.19.68.222	208.71.166.109

Australia SBC IPs.

Melbourne (Primary Site)	Sydney (Secondary Site)
202.147.130.82	202.147.130.90

Melbourne PCI (Primary Site)	Sydney PCI (Secondary Site)
202.147.129.156	202.147.130.93

UK SBC IPs.

Primary AZ	Secondary AZ
34.255.92.105	52.211.77.33

Canada SBC IPs.

Primary AZ	Secondary AZ
primary.sip.ca.inferencecommunications.com 99.79.86.10	secondary.sip.ca.inferencecommunications.com 99.79.121.161

Media Server Public IP Addresses

USA Virginia Media Server Public IPs.

IP Addresses
104.37.106.48/28
199.19.68.208/28

USA Chicago Media Server Public IPs.

IP Address
199.189.190.64/28

AUS Melbourne Media Server Public IPs.

IP Address
202.147.137.0/28

AUS Sydney Media Server Public IPs.

IP Address
202.147.139.16/28

UK Media Proxy IPs.

Primary	Secondary
52.18.167.135	34.246.159.75

Canada Media Proxy IPs.

Primary	Secondary
99.79.92.109	52.60.164.146

Network

Five9 Network Connectivity

Five9 Customers have multiple Wide Area Network (WAN) Options available to connect directly and securely into the Five9 Data Centers. Depending on the option selected, a customer may have to install networking equipment such as a Router or Firewall within the Five9 Data Center. This equipment will be managed by the customer and be connected into the Five9 Infrastructure through an RJ45 Ethernet Connection.

Virtual Private Network (VPN)

For customers that prefer to establish a direct connection to the Five9 data center to enhance the security of voice and data transmission over the Internet, Five9 offers a VPN Option. For an additional monthly fee, Five9 can support a Site-to-Site connection to any industry-standard VPN solution, providing secure encrypted transmission of all voice and data. Please note the bandwidth requirements in Bandwidth Requirements when using the VPN option.

VPN and Quality of Service (QOS)

Direct connections, such as MPLS or Ethernet-based services, provide enhanced Quality of Service (QoS). Although most direct connections include a QoS guarantee, the standard of quality is no greater than that achieved by Tier1 Internet Service Providers

because these providers offer low network latency. Additionally, to ensure sufficient quality of service for VoIP calls, you can use a separate Internet connection for VPN or give VPN traffic highest priority in your network.

VPN and Private IP Addresses

Most companies are using VPN for site-to-site connectivity by encapsulating traffic with private IP addresses (RFC 1918). This could be done on both sides of a VPN tunnel if both sides of the tunnel are under control of the same company.

If a VPN tunnel exists between your premises and a Five9 data center, all traffic traveling across the VPN tunnel should be routable by all Five9 VCC equipment. This requires that all such traffic must use public IP addresses. If you plan to use a VPN, apply Network Address Translation (NAT) to any traffic going inside VPN tunnel using public IP addresses.

Direct Connection Option

Five9 data center Internet connections provide 20 times more bandwidth than the average usage and three times the fault tolerance. In most cases, using the public Internet as a transport between the customer's and Five9 networks provides more than enough bandwidth. The limiting factor is usually the last mile connection to your premises. If you are required to establish a direct connection to a Five9 data center, such as through MPLS, the Five9 Direct Connection option provides this capability.

Direct Connection can be used as an alternative to VPN option. Direct Connection is useful if you want greater control over bandwidth and QoS for VoIP.

Required Direct Connection Criteria

You are responsible for establishing a leased line connection to a Five9 data center and for providing 10/100/1000MB full-duplex Ethernet hand-off to connect to Five9 network equipment.

Important

The hand-off must be Layer-3, and the port must not have Layer-2 capabilities.

All traffic coming through the leased line will use NAT to a publicly routable IP address or a private IP address assigned to the LAN interface of the network router terminating the connection.

To reroute traffic across the Internet or another dedicated connection in case of a dedicated link equipment failure, you should establish a failover mechanism, such as Border Gateway Protocol (BGP).

WebRTC

WebRTC (Web Real-Time Communication) enables agents to communicate with customers from their browser. Agents do not need to install the softphone plug-in and an extension because audio and video communication are inside web pages. Not all agents in your domain need to use WebRTC. Agents can use the softphone as needed.

WebRTC is available on Plus applications for customers with Agents hosted in North America data centers as well as in FGV POPs.

Requirements	Description
Five9 Voice Service (FVS)	Domain enabled
Five9 Plus applications	Supervisor Plus, Agent Desktop Plus, and Plus CRM adapters.
WebRTC	Domain enabled
VDI	Citrix/VMWare Horizon desktop client **Limitation in Chrome (Windows)**: The agent's audio devices cannot be detected. As a workaround, disable audio sandbox manually or in GPU.
Firewall	• UDP outbound ports: 1024–65535 RTP between Five9 applications. If you do not use a stateful firewall, configure inbound rules to allow return traffic. All ports open for RTP must also allow STUN. • TCP outbound port: 443 HTTPS-web communications for login, reporting, and customer support.
Public IP addresses for Five9 Global	• Canada (MTL103) WebSocket/agent registration: 74.114.193.24

Requirements	Description
Voice POPs	• Canada (MTL10) WebSocket/agent registration: 74.114.192.24 • Sao Paulo WebSocket/agent registration: 18.229.177.118 Media: 18.228.254.135 Media: 18.230.128.58 • Sydney WebSocket/agent registration: 13.211.19.119 Media: 52.64.122.16 Media: 3.105.60.140 • Tokyo WebSocket/agent registration: 3.115.80.118 Media: 18.180.1.110 Media: 54.248.166.76

For more information about this connection option, contact your Five9 representative.

Five9 Network Requirements (LAN and WAN)

Five9 recommends the following bandwidth for each of the listed usage scenarios:

> **Note**
> These values apply to the G.711 codec, which is used by default. G.711 provides an uncompressed high quality voice.

Five9 Bandwidth Requirements

These requirements apply to each agent.

Usage	Minimum	Recommended
Five9 Agent Desktop Plus and Plus adapters	128 kbps	128 kbps
Five9 Agent standalone (Java)	88 kbps	88 kbps
Five9 Agent with light web browsing	112 kbps	128 kbps
Five9 Agent Assist	12 kbps	12 kbps [1]
VPN connectivity	Additional 64 kbps	Additional 64 kbps
Business applications, such as on-demand CRM software	Additional 64 kbps	Additional 64 kbps
Five9 UC - Skype for Business	12 kbps	12 kbps
Five9 UC - Microsoft Teams	320 kbps	320 kbps
Five9 UC - Zoom	320 kbps	320 kbps
Five9 UC - Office@Hand	320 kbps	320 kbps
Five9 UC - RingCentral	320 kbps	320 kbps
Other Five9 users and services, such as administrators, supervisors, FTP, and reports	As needed	As needed

[1] Five9 Agent Assist application requires 12 kbps bandwidth in addition to Agent application.

Five9 Network Recommendations

Connection Type	Support Details
Latency	Latency from the customer system to the Five9 Data center must be under 150ms one-way. Faster networks perform better. Internet connections from outside the United States are subject to higher latency, which can affect the Quality of Service (QoS).
Wireless LANs	Wireless Local Area Networks (LANs) are not supported for multi-user environments. Wireless may be used in a single user environment if the agent station is the only wireless device in use. However voice quality may be compromised. Five9 recommends wired connections for best results.
Satellite and Wireless Internet	Satellite and wireless connections are not supported.
SIP and RTP Traffic	Do not restrict SIP and RTP traffic across LANs and/or WANs when multiple customer sites exist.

Connection Type	Support Details
NAT and PAT	NAT and/or PAT are supported configurations. Double Network Address Translation (Double NAT) is not supported.

Bandwidth Requirements for Five9 Video Engagement for Agents

A stream that includes audio, video, and sharing ranges from 100 to 500 kbps, depending on your network capacity, movement, light, and camera. Five 9 recommends to validate the network capacity before intensive use.

Video Size	Audio Only	Thumbnail	Mid Size	Full Screen
1:1 HD Resolution		320 x 180	640 x 360	1280 x 720
1:1 HD Quality	30 Kbps	130 Kbps	280 Kbps	560 Kbps
1:1 HD Resolution		160 x 90	320 x 180	640 x 360
1:1 HD Quality	30 Kbps	80 Kbps	130 Kbps	280 Kbps

Multi-Party				
Conference Active Speaker HD	30 Kbps	280 Kbps	280 Kbps	280 Kbps
Conference Active Speaker HD	30 Kbps	130 Kbps	130 Kbps	130 Kbps
Conference Additional Passive Speaker*	0 Kbps	+40 Kbps	+40 Kbps	+40 Kbps
**Video conferences support the display of four passive speakers. Attendees can join a conference in addition to the active speaker and on-screen passive speakers.*				

Screen Sharing				
Maximum Resolution	2560 x 1600	2560 x 1600	2560 x 1600	2560 x 1600
Additional Bandwidth	+20 Kbps	+20 Kbps	+20 Kbps	+20 Kbps

Other VoIP Services and Phones, Ports, IP Address Ranges, and Network Traffic

Other VoIP (Voice over Internet Protocol) Services and phones should be on a network segment separate from the Five9 workstation firewall requirements. Communication to Five9 is done through standard DNS requests. Agent desktops should resolve all server names for Five9.com domain.

The URL standard contains a port specification. For example: www.domain.com means http://www.domain.com:80. The default port is generally omitted. Five9 URLs do not use a port other than 80.

Five9 uses certain TCP/UDP ports for Five9 applications and communications. Customers must avoid using the following TCP/UDP ports for any third-party services or applications running on agent desktop computers: 8080, 9998, 11000, 30059.

Five9 recommends that you configure your firewall to allow traffic only at the TCP/ UDP ports and source destination to or from any of the Five9 data center IP address ranges/internet domains listed in this section.

Five9 Internet Domains and IP Addresses

Ensure that you add Five9 Internet domains and IP addresses to your list of allowed domains and IP addresses. You may add IP addresses to your list at several points in your network. Be sure that IP address restrictions defined in your firewall match the Five9 IP address ranges and domains listed here. The list of allowed entities overrides SPAM filters and lists of denied entities.

Five9 IP Address Ranges

To avoid potential service impacts, you must add Five9 IP addresses to a list of allowed entities in your IPS solutions.

> **Note**
> If your network security protocols restrict the external IP addresses that you can use, contact your Five9 representative for assistance in configuring Five9 email.

If you use Microsoft Exchange 2010, email delivery to your users may be delayed unless you set the value of `MaxAcknowledgementDelay` to 1 second.

US IP Ranges	Location of Data Center	CIDR Format
38.107.71.0 – 38.107.71.255	Santa Clara	38.107.71.0/24
147.124.160.0 – 147.124.191.255		147.124.160.0/19
162.213.152.0 – 162.213.153.255		162.213.152.0/23
198.105.200.0 – 198.105.201.255		198.105.200.0/23
198.105.206.0 – 198.105.206.255		198.105.206.0/24
147.124.160.0 – 147.124.191.255	Atlanta	147.124.160.0/19
198.105.202.0 – 198.105.203.255		198.105.202.0/23
198.105.207.0 – 198.105.207.255		198.105.207.0/24
208.69.28.0 - 208.69.29.255		208.69.28.0/23
In the US, other data centers are optional.		

Canada IP Ranges (Montreal)	Location of Data Center	CIDR Format
74.114.192.0 – 74.114.193.255		74.114.192.0/23
34.95.54.0 - 34.95.54.63		34.95.54.0/26
34.95.20.197	login.five9.ca	

Canada IP Ranges (Montreal)	Location of Data Center	CIDR Format
35.203.62.218		
34.95.47.32 35.203.0.33	api.five9.ca	
35.203.103.232 34.95.57.4	app.ca.five9.com	
35.203.103.118	a1.ca.five9.com	
35.203.54.96	ca2.ca.five9.com	
35.203.63.204	core001-204.mtl2.ca.five9.com	
35.203.127.202	core001-1.mtl.ca.five9.com	
34.95.41.230	env001-1.mtl1.ca.five9.com	
34.95.57.222	env001-204.mtl2.ca.five9.com	
147.124.160.0 – 147.124.191.255		147.124.160.0/19
35.203.53.138	verint06.five9-wfo.com (Verint Application Suite)	
34.95.53.189	v06-ris-01-301.five9-wfo.com	
35.203.69.68	v06-ris-01-401.five9-wfo.com	
34.95.32.12	v06-sr-01-301.five9-wfo.com	
35.203.76.88	v06-sr-01-401.five9-wfo.com	
In Canada, other data centers are optional.		

EU IP Ranges	Location of Data Center	CIDR Format
185.111.40.0 – 185.111.41.255 212.187.211.0 – 212.187.211.255 147.189.16.0 – 147.189.31.255 147.189.224.0 – 147.189.239.255	London	185.111.40.0/23 212.187.211.0/24 147.189.16.0/20 147.189.224.0/20
34.89.67.64 - 34.89.67.127	London GCP	34.89.67.64/26
35.246.110.38 34.105.236.95 34.89.67.65 34.89.67.66	London GCP Verint	

EU IP Ranges	Location of Data Center	CIDR Format
34.89.67.72 34.89.67.73 34.89.67.74 34.89.67.75 34.89.67.76 34.89.67.77		
34.105.236.95 and 34.89.24.240	Network Assessment Tool	
5.175.80.160 – 5.175.80.175 94.103.30.32 – 94.103.30.63 94.103.30.144 – 94.103.30.159 94.103.30.160 – 94.103.30.175 185.111.42.0 – 185.111.43.255 147.189.16.0 – 147.189.31.255 147.189.224.0 – 147.189.239.255	Amsterdam	5.175.80.160/28 94.103.30.32/27 94.103.30.144/28 94.103.30.160/28 185.111.42.0/23 147.189.16.0/20 147.189.224.0/20
In the EU, other data centers are optional.		

Note

Intrusion Prevention Systems (IPS) solutions are designed to block real-time traffic that matches certain attack behavior. Because every IPS solution responds to traffic differently, and you may receive daily updates to attack signatures, the behavior of IPS solutions can be unpredictable. False positives are possible.

If your IPS overreacts to normal VOIP (SIP and RTP) traffic to and from Five9, you may experience service interruptions.

Five9 IP Addresses for Global Voice

These production IP addresses apply only to Five9 Global Voice.

Location	IP Address
Dublin	34.241.191.251
Sao Paolo	18.231.8.114
Sydney	52.63.91.200
Tokyo	54.64.27.35

Five9 IP Addresses for Email

Location of Data Center	IP Addresses
Santa Clara	198.105.204.18
	198.105.204.19
	198.105.204.20
Atlanta	198.105.205.18
	198.105.205.19
	198.105.205.20
London	185.49.234.25
	185.49.234.29
	185.49.234.30
Amsterdam	94.103.30.47
	94.103.30.53
	94.103.30.54
Canada and London GCP	87.253.232.0 – 87.253.239.255
	185.189.236.0 – 185.189.239.255
	185.211.120.0 – 185.211.123.255
	185.250.236.0 – 185.250.239.255

Five9 Connectivity Assessment Test

These production IP addresses apply only to Connectivity Assessment Test.

Servers	IP Addresses
CAT Servers	198.105.200.22 – 198.105.200.25
	198.105.202.16 – 198.105.202.18
	198.105.202.9
	212.187.211.5 – 212.187.211.6
	38.107.71.103
Cloud CAT Servers	52.196.118.63
	3.105.227.19
	18.229.56.203
	108.129.62.47
	35.203.75.94
	94.103.30.146-147

Five9 IP Addresses for Callback API Integration

If you implement API integrations with Five9 services and require Callback API integration, ensure that you add the following IP addresses to your IP allow list.

Location	IP Address
US	35.231.25.195 34.70.24.218 35.243.214.240 34.66.82.195 35.229.109.107 34.71.1.196 35.185.70.123 35.192.111.252 104.196.65.187 146.148.69.156
EU	34.91.242.131 34.78.235.107 34.90.189.196 35.187.71.103 35.246.33.168

Five9 Internet Domains

All communication and content from Five9 originates from one of these domains. Therefore, be sure to add them to your list of allowed entities.

Five9 Domain	Data Center	URL
five9.com www.five9.com	U.S. data centers	• `https://login.five9.com` • `https://app.five9.com` • `https://app-scl.five9.com` • `https://app-atl.five9.com` • `https://us1.five9.com` • `https://us8.five9.com` • `https://us6.five9.com` • `https://us9.five9.com` • `https://webstatic.five9.com`

Five9 Domain	Data Center	URL
		• https://ws1.five9.com • https://ws8.five9.com • https://ws6.five9.com • https://ws9.five9.com • https://us.five9.net • https://api.prod.us.five9.net • https://cdn.prod.us.five9.net • https://login.auth.five9.com • https://auth.five9.com • https://sso1.auth.five9.com • https://migrate.sso1.auth.five9.com • https://portal.five9.com • https://admin.five9.com
five9.ca www.five9.ca	Canada data center	• https://login.five9.ca • https://ca1.ca.five9.com • https://ca2.ca.five9.com • https://api.five9.ca • https://app.ca.five9.com • https://app-mtl1.ca.five9.com • https://core001-204.mt12.ca.five9.com • https://core001-1.mt11.ca.five9.com • https://env001-204.mt12.ca.five9.com • https://env001-1.mt11.ca.five9.com • https://env001-204.mtl2.ca.five9.com • https://ca.five9.net • https://api.prod.ca.five9.net • https://cdn.prod.ca.five9.net
five9.eu www.five9.eu	European data centers	• https://login.five9.eu • https://app-ldn.five9.eu • https://app-ams.five9.eu • https://eu1.five9.eu • https://eu2.five9.eu • https://eu3.five9.eu

Five9 Domain	Data Center	URL
		• https://eu4.five9.eu • https://webstatic.five9.eu • https://ws1.five9.eu • https://ws2.five9.eu • https://ws3.five9.eu • https://ws4.five9.eu • https://webstorage01.five9.eu • https://webstorage02.five9.eu • https://webstorage03.five9.eu • https://webstorage04.five9.eu • https://eu.five9.net • https://api.prod.eu.five9.net • https://cdn.prod.eu.five9.net • https://login.auth.five9.eu • https://auth.five9.eu • https://sso1.auth.five9.eu • https://migrate.sso1.auth.five9.eu • https://portal.five9.eu • https://admin.five9.eu
Five9 UC - Microsoft Teams	U.S. data centers	• https://graph.microsoft.com/v1.0/groups • https://graph.microsoft.com/v1.0/groups/<id>/members • https://graph.microsoft.com/beta/communications/getPresencesByUserId • https://graph.microsoft.com/beta/groups?$filter=resourceProvisioningOptions/Any(x:x eq 'Team')
Five9 UC - Zoom	U.S data centers	• https://api.prod.us.five9.net
Five9 UC - Office@Hand	U.S data centers	• https://api.prod.us.five9.net
Five9 UC - Skype for Business		• https://latest-swx.cdn.skype.com/ • https://swx.cdn.skype.com Add these domains to your list of allowed entities for your Skype or Lync instance:

Five9 Domain	Data Center	URL
		• https://app.five9.com* • https://app-atl.five9.com* • https://app-scl.five9.com* • https://app-ldn.five9.com* • https://app-ams.five9.com*
Digital Engagement administrator console for Plus and Java agent applications	• Santa Clara • Atlanta • London • Amsterdam	• https://us8.five9.com/SoCoCare/AdminConsole/# • https://us9.five9.com/SoCoCare/AdminConsole/# • https://eu1.five9.eu/SoCoCare/AdminConsole/# • https://eu2.five9.eu/SoCoCare/AdminConsole/# Ensure that you are using the correct chat console for your agent interface: • Web-based console for web-based agents • Java-based console for Java-based agents. Contact your Five9 representative if you have questions.
Connectivity Assessment Testing	CAT web site	• https://www.five9.com/cat • https://download.visualware.com

CounterPath Softphone Requirements

Five9 uses the CounterPath softphone client. You must ensure that Five9 agents and API connections can contact the CounterPath License Server for validation. Depending on your firewall configuration, use one of these methods:

- Create a firewall rule to permit HTTPS connections to secure.counterpath.com.

  or

- If you specify firewall exceptions with IP addresses instead of DNS, add these IP addresses to your list of allowed entities:

69.90.51.170	secure.counterpath.com
216.93.246.170	secure.counterpath.com
137.135.52.175	secure.counterpath.com

Performance Dashboard

To access Performance Dashboard, you must add to your list of allowed entities in your servers the domain and sub-domains of `clearviewportal.com`:

- ***<your_domain>***`.clearviewportal.com`
- `clearviewwebhostuc1b.clearviewportal.com`
- `uc1b-mod.clearviewportal.com`
- `uc1b-mod-rt.clearviewportal.com`

ClearView is hosted by CenturyLink Cloud. For more information, contact your Five9 representative.

SIP Firewall Note

Many firewalls with default inspect settings make changes to SIP/VoIP traffic. In most cases intrusive inspection by the Firewall changes the SIP VoIP traffic and is unnecessary for Five9 applications. The following SIP Inspections should be turned off for Five9 traffic:

- SIP Access Layer Gateway (ALG)
- SIP Inspection and Control
- SIP Traversal
- SIP Transformation

Note

You might be running multiple SIP services and other applications which require these features to be enabled.

TCP/UDP Port Requirements for Softphone Customers

If your agents use a softphone connection, these TCP and UDP ports must allow traffic in your external firewall, Session Border Controller (SBC), SIP proxy, and firewall of workstations:

Port	TCP/UDP	Outbound	Application
80	TCP	Outbound	HTTP web communications for login, reporting, customer support.

Port	TCP/UDP	Outbound	Application
443	TCP	Outbound	HTTPS web communications for login, reporting, customer support.
1024-65535	UDP	Outbound	RTP between Five9 applications. If you are not using a stateful firewall, you must configure inbound rules to allow return traffic.
2200-2300	TCP	Outbound	Java RMI encrypted.
5060-5067	UDP	Outbound	SIP connection for the agent application.
5080	UDP	Outbound	SIP signaling on the Five9 SIP proxy.
5081	TCP	Outbound	SIP over TLS signaling on the Five9 SIP proxy.
8000-8015	UDP	Outbound	Source port used for RTP traffic on the agent desktop.
8080/8081	TCP	Outbound	Network Assessment Test (NAT) used by `quality.five9.com` to verify that your networks are ready to receive Five9 traffic.
8083	TCP		Used by Five9 Softphone Service. Ensure that no other processes use this port in the agents' workstations. Does not need to be open in the network firewall but needs to be open if a host firewall exists. If you plan to use a proxy, create an exception for this port. Otherwise, the softphone connection will fail. For instructions, see *Installing the Five9 Softphone for Plus Applications* in the Basic Configuration Administrator's Guide.
8843	TCP	Outbound	HTTPS Downloading Five9 applications and API.
8880	TCP	Outbound	HTTP Downloading Five9 applications.

TCP/UDP Port Requirements for Gateway Customers

If your agents use a gateway phone connection, these TCP and UDP ports must allow traffic in your external firewall, Session Border Controller (SBC), SIP Proxy, and workstations firewall:

Port	TCP/UDP	In or Out	Application
80	TCP	Outbound	HTTP web communications necessary for login,

Port	TCP/UDP	In or Out	Application
			reporting, customer support.
443	TCP	Outbound	HTTPS web communications necessary for login, reporting, customer support.
1024-65535	UDP	Outbound	RTP from Five9 Agent Desktop to Five9 Application. **Note:** If you are not using a stateful firewall, you MUST configure Inbound rules to allow return traffic.
2200-2300	TCP	Outbound	Java RMI encrypted.
5060	UDP	Inbound	SIP connection for Five9 Agent Default is 5060; the actual port number used depends on what the customer is using for their SIP endpoint.
5080	UDP	Outbound	SIP signaling on the Five9 SIP Proxy.
5081	TCP	Outbound	SIP over TLS signaling on the Five9 SIP Proxy.
8080/8081	TCP	Outbound	Network Assessment Test (NAT); Used for the quality.five9.com site to verify that customer network is ready to receive Five9 traffic.
8843	TCP	Outbound	HTTPS Downloading Five9 applications and API.
8880	TCP	Outbound	HTTP Downloading Five9 applications.

TCP/UDP Port Requirements for PSTN Customers

If your agents use a PSTN connection but no RTP connection is required, be sure that these TCP and UDP ports allow traffic in your external firewall, Session Border Controller (SBC), SIP Proxy and, workstations firewall:

Port	TCP/UDP	In or Out	Application
80	TCP	Outbound	HTTP web communications necessary for login, reporting, customer support.
443	TCP	Outbound	HTTPS web communications necessary for login, reporting, customer support.
2200–2300	TCP	Outbound	Java RMI encrypted.
8080/8081	TCP	Outbound	Network Assessment Test (NAT).
8090	UDP	Outbound	Used for Voice Simulation tests.
8843	TCP	Outbound	HTTPS Downloading Five9 applications and API.
8880	TCP	Outbound	HTTP Downloading Five9 applications.

TCP and UDP Ports for Connectivity Assessment Test

These ports must allow traffic in the your external firewall, Session Border Controller (SBC), SIP Proxy, and workstations firewall:

Port	TCP/UDP	In or Out	Application
80	TCP	Outbound	HTTP connection and communication for server-client traffic, test data transfer and error reporting.
443	TCP	Outbound	HTTPS connection.
5060	TCP	Outbound	SIP simulation port.
5060	UDP	Outbound	SIP simulation port.
8080–8081	TCP	Outbound	Connectivity assessment reserve test ports.
8090	UDP	Outbound	Capacity and bandwidth testing port.
20000–20001	TCP	Outbound	Speed download and upload testing Ports.
20000–20001	UDP	In or Out	VoIP download and upload testing ports.

TCP Port Requirements for FTP/SFTP

If you use `ftp.five9.com` to upload call recordings or download dialing lists, you must configure your external firewall to allow traffic on these ports:

Port	TCP/UDP	Outbound	Application
21	TCP	Inbound	To download dialing lists from your FTP server specified in VCC Configuration. Use FTP helper in firewall configuration to open FTP-DATA communications.
21	TCP	Outbound	To upload call recordings to your FTP server specified in VCC configuration. Use FTP helper in firewall configuration to open FTP-DATA communications.
22	TCP	Inbound	To download dialing lists (by using SFTP) from your SFTP server specified in VCC Configuration.
22	TCP	Outbound	To upload call recordings (by using SFTP) to your SFTP server specified in VCC Configuration.

Network Requirements for Five9 Video Engagement

To enable agents to connect to the platform, configure these ports and domains:

If you use the RTCC driver	• Port TCP 80 (HTTP) • Port TCP 443 (HTTPS)
If you use WebRTC *This section is unrelated to the WebRTC section earlier in this chapter.*	• Port TCP 80 (HTTP) • Port TCP 443 (HTTPS) • Port TCP 444

You must also add these wildcard URLs to your list of allowed URLs:

- `*.rtccloud.net`: Web connection plug-in
- `*.sightcall.com`: Access agent console interface
- `*.mapbox.com`: Third-party library for geolocation

Port Requirements for Email

Five9 supports IMAP and POP3 protocols for inbound email, and SMTP protocol for outbound email. The table below lists the default ports for these protocols.

To use Five9 Digital Engagement Email, Five9 IP Addresses for Email require access to the applicable ports below or to the non-default ports where your inbound or outbound mail service is provided.

Traffic	Protocol	Ports
Inbound	IMAP, IMAP Secure	143: Not encrypted 993: Secure
	POP3/POP3 Secure	110: Not encrypted 995: Secure
Outbound	SMTP	465: Secure 587: Encrypted (STARTTLS) [1]

[1] When port 587 is used for outbound, STARTTLS is used to ensure encryption of the communication between the client and the SMTP service, provided the SMTP service supports StartTLS. For other ports, SSL is used, and if SSL connection fails, then STARTTLS is used. If both connections fail, then the connection is tried without SSL or TLS.

SOAP APIs

For SOAP APIs, your external firewall needs to allow outbound connections on TCP Port 8843 from the computer using the API web services to the Five9 data center subnets.

For CTI Web Services, if you use Agent Desktop Toolkit, the TCP/UDP Port requirements listed in this document for softphone, gateway or PSTN customers may apply.

Third-Party Software

Consult your CRM vendor's technical documentation or customer support for details about the domains in use with the respective applications.

Five9 Quality of Service (QoS) Features

To prioritize voice traffic in a converged voice/data network, Five9 VCC uses Diffserv QoS (Quality of Service) markings of SIP and RTP network packets for VoIP phone calls. Five9 VCC uses the following ports that can be used by your internal networking engineering team to add to an existing QoS policy or develop a custom policy:

Protocol	Requirements
RTP	Highest priority, low latency queue across the network infrastructure. Source Ports: UDP 8000—8015 Destination Ports: UDP 1025—65535
SIP	Can be in the highest priority queue but may also be in a second queue less critical than RTP. Source Port: UDP 5060 Destination Port: UDP 5080

Five9 VCC marks the SIP and RTP network packets for VoIP calls that are leaving Five9 destined for the customer or provider network. Five9 VCC does not mark the DSCP header on packets leaving the workstation destined for the Five9 network. Five9 recommends that the network protocols defined for this purpose be marked and prioritized by the workstation or the network infrastructure.

Workstation QoS Option

To enable VoIP QoS for your agents' workstations, Five9 recommends that you set up a Windows QoS policy. For more information, refer to these articles: MSDN article

(Creating and Editing a QoS Policy) and TechNet article (QoS Support in Windows).

Network QoS Option

To enable VoIP QoS tagging on the network infrastructure equipment, consult your networking equipment vendor and/or an internal network engineer in your company.

Workforce Optimization Requirements

The Five9 Workforce Optimization (WFO) integration enables Five9 VCC to share various data elements with the WFO Quality Monitoring (QM) and Workforce Management (WFM) solutions.

The following sections describe the Workforce Optimization product requirements for use with Five9 VCC.

Agent Workstation Requirements

The following requirements assume that the Five9 VCC and Workforce Optimization (WFO) agent client products are the only software applications running in the agent workstation environment. Agents who use additional resource-intensive application require additional resources, such as additional RAM, HDD I/O, and CPU. A system administrator should determine the resources necessary to support all agent applications.

Virtualized Agent Environments

QM screen capture is supported on Virtual Desktop Infrastructure (VDI) or thin-client deployments accessing applications by using terminal services. For more information, see QM documentation.

Hardware

Component	Minimum Requirement	Notes
Processor	Dual-Core CPU. 2M Cache, 1.8 GHz, 800 MHz FSB.	No manufacturer required.
Memory	2.0 GB	4.0 GB recommended for Windows Vista or later.
Architecture	32-bit or 64-bit supported	
Hard Disk	7200 RPM SATA HDD 2GB free required 10 GB free space required[1] 20 GB free space preferred[1]	Cache of captured screen media resides locally on agent workstation. Configuration of solution-specific options for local cache are available.
Audio Devices	Windows standard audio output device Applicable device drivers	Headphones or speakers are required for media playback.

[1] Required only by QM Screen Capture.

Operating Systems

Operating System	Version (32- and 64-bit)
Windows Vista	Service Pack 2.
Windows 10 Home, Pro, Enterprise	Latest release.

Web Browsers

The following web browsers are supported for all WFO components.

Browser	Version (32-bit)
Google Chrome	Latest release.
Firefox	Latest release.
Edge	Latest release.
Safari	Latest release.
Internet Explorer	Version 9 or higher.

Software Requirements

Component	Requirement
Windows Media Player	Version 9 or higher.

Configuration Requirements

Component	Requirement
Local Permissions	Configuration of Full Control permission to local application installation directory is required if agents are not administrative users of their PCs.
Windows User Account Control	Use of User Account Control is compatible. An administrative user, bypassing UAC, is required for the successful installation and configuration of the client, whether configuration is completed locally on the PC or by an automated deployment method.
Local Firewall	Exceptions to local Windows Firewall policies may be required depending on site-specific policies. For more information, see deployment instructions.
Local Anti-Virus or Anti-Malware	Exceptions to local anti-virus or malware detection applications may be required depending on site-specific policies. Add the following executables in any anti-virus or anti-malware program: • <Installation Directory>\voacli.exe • <Installation Directory>\voacld.exe • <Installation Directory>\voacsc.exe • <Installation Directory>\voacmt.exe • <Installation Directory>\voacse.exe • <Installation Directory>\voaclm.exe • <Installation Directory>\RC\voacvc.exe

Firewall Policies

Source	Destination	Port	Protocol	Description
Agent PC [1]	WFO CLOUD	443	TCP	Screen capture clien HTTPS heartbeat messaging.
Agent PC [1]	WFO CLOUD	22	TCP	Screen capture FTP file transfer.
Agent PC	WFO CLOUD	443	TCP	Application Access.
Agent PC [2]	WFO CLOUD	5018	TCP	Live Agent Desktop Access.
Agent PC [2]	WFO CLOUD	5019	TCP	Live Agent Desktop Access.

[1] Required only by QM Screen Capture.

[2] Required only by QM Live Desktop.

Supervisor Workstation Requirements

The following requirements assume that the Five9 VCC and Workforce Optimization (WFO) agent client products are the only software applications running in the agent workstation environment. Agents who use additional resource-intensive application require additional resources, such as additional RAM, HDD I/O, and CPU. A system administrator should determine the resources necessary to support all agent applications.

Virtualized Supervisor Environments

QM Supervisor access is supported with Virtual Desktop Infrastructure (VDI) or thin-client deployments accessing applications by using terminal services. For more information, see QM documentation.

Hardware

Component	Minimum Requirement	Notes
Processor	Dual-Core CPU. 2M Cache, 1.8 GHz, 800 MHz FSB.	No manufacturer required.
Memory	2.0 GB	4.0 GB recommended for Windows Vista or later.
Architecture	32-bit or 64-bit supported	
Hard Disk	7200 RPM SATA HDD 2GB free required 10 GB free space required[1] 20 GB free space preferred[1]	Cache of captured screen media resides locally on agent workstation. Configuration of solution-specific options for local cache are available.
Audio Devices	Windows standard audio output device Applicable device drivers	Headphones or speakers are required for media playback.

[1] Required only by QM Screen Capture.

Operating Systems

Operating System	Version (32- and 64-bit)
Windows Vista	Service Pack 2.
Windows 10 Home, Pro, Enterprise	Latest release.

Web Browsers

The following web browsers are supported for all WFO components.

Browser	Version (32-bit)
Google Chrome	Latest release.
Firefox	Versions 52 and 53.

Browser	Version (32-bit)
Edge	Latest release.
Safari	Latest release.
Internet Explorer	Version 9 or higher.

Software Requirements

Component	Requirement
Windows Media Player	Version 9 or higher

Configuration Requirements

Component	Requirement
Local Firewall	Exceptions to local Windows Firewall policies may be required depending on site-specific policies. See deployment instructions for further detail.
Local Anti-Virus or Anti-Malware	Exceptions to local AV or malware detection applications may be required depending on site-specific policies. Add the following executables in any anti-virus or anti-malware program: • <Installation Directory>\voacli.exe • <Installation Directory>\voacld.exe • <Installation Directory>\voacsc.exe • <Installation Directory>\voacmt.exe • <Installation Directory>\voacse.exe • <Installation Directory>\voaclm.exe • <Installation Directory>\RC\voacvc.exe

Firewall Policies

Source	Destination	Port	Protocol	Description
Supervisor PC	WFO CLOUD	443	TCP	Application Access.

Bandwidth Considerations

Internet bandwidth is used by Five9 Workforce Optimization (WFO) by two primary mechanisms.

User playback of media in Quality Monitoring (QM) uses bandwidth, whether by a supervisor or agent. In this scenario, media is streamed from the WFO cloud environment to the user workstation.

Screen capture uses bandwidth when screen cache data is moved from the agent premise to the WFO cloud environment.

User Media Playback

Playback Type	Playback Bandwidth Rate
Audio Only	100 KBps
Audio & Screen Capture (1 monitor)	300 KBps
Audio & Screen Capture (2 monitors)	600 KBps
Audio & Screen Capture (3 monitors)	900 KBps

Screen Capture Cache Transmission

Capture Type	Average Data Transmission, Per Minute Recorded	Average Transmission Rate
1 Monitor	1.5 MB	1500 KBps
2 Monitors	2.0 MB	1500 KBps
3 Monitors	3.0 MB	1500 KBps

Screen capture usage estimates are provided for initial sizing only. Actual usage can vary greatly depending on screen content, activity, monitor resolution, and other environmental factors. Five9 recommends that for site-specific bandwidth usage metrics, run a pilot group test during deployment.

Example Screen Capture Calculation

The following expression can be used for screen capture calculation.

```
Number of Agents (x) Monitors for each computer(x) Minutes Recorded (x)
Data Transmission Size = Total Daily Upload
```

Example

50 agents (x) 2 monitors (x) 18,000 minutes recorded per day (x) 2.0 MB per minute captured = 3.5 GB upload per day

References

Glossary

Term/Acronym	Definition
ACL	Lists that filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. Your router examines each packet to determine whether to forward or drop the packet, based on the criteria you specified within the access lists.
Codec	Codecs are used to convert an analog voice signal to digitally encoded version. Codecs vary in sound quality and bandwidth required.
CTI	Computer Telephony Integration.
Diffserv QoS	Differentiated Services (Diffserv) QoS framework enables quality-of-service provisioning in a network domain by applying rules at the edges to create traffic aggregates and by coupling each of these with a specific forwarding path treatment in the domain through use of a code point in the IP header.
Digital Certificate	Digital Certificates provide a means of proving identity in electronic transactions. Also known as a public key certificate, the digital certificate is an electronic document that uses digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
G.711	Two main VoIP compression algorithms: • µ-law algorithm is used in North America & Japan. • A-law algorithm is used in the rest of the world. The sample rate is 64 kbit/s bit.
G.729	ITU standard codec with two main versions: A and B. For VoIP processing, the sample rate ranges from 28 to 40kbit/s bit, depending on overhead.

Term/Acronym	Definition
MPLS	Multiprotocol Label Switching (MPLS) is a pure IP architecture that combines the strengths of Layer-3 routing and Layer-2 switching. MPLS carrier networks are scalable virtual private networks (VPNs) that provide end-to-end quality of service (QoS).
NAT	Network Address Translation translates IP addresses used in one network to a different IP address known to another network.
PAT	Port Address Translation works with NAT to conserve IP addresses used by permitting multiple devices on a local area network (LAN) to be mapped to a single IP address.
RTP protocol	Real-Time Transport is used with the RTP Control Protocol (RTCP). RTP carries the media streams, such as audio and video whereas RTCP monitors transmission statistics and quality of service (QoS) and helps to synchronize multiple streams. With WebRTC, STUN protocol messages are sent through these ports.
SBC	Session Border Controller (SBC) is a device deployed in Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually the media streams involved in setting up, conducting, and tearing down SIP calls.
SIP	Session Initiation Protocol works in the Application Layer to control communications for video, voice, IP, unicast, and multicast sessions.
SIP ALG	SIP-ALG is a firewall that can perform NAT with standard SIP protocols.
SIP Inspection	To support SIP calls through the security appliance, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user-data portion of the IP packet. SIP inspection applies NAT for these embedded IP addresses.
SIP Trunking	SIP trunks are VoIP-based carrier services based on the Session Initiation Protocol (SIP) by which Internet telephony service providers (ITSPs) deliver telephony PSTN Services.
STUN protocol	Session Traversal Utilities for NAT is a Network Address Translator (NAT) traversal tool for other protocols. STUN can be used by an endpoint to determine the IP address and port allocated to it by a NAT.
TCP/UDP Ports	Transport Layer protocols, such as Transmission Control Protocol (TCP), the User Datagram Protocol (UDP); specify a source and

Term/Acronym	Definition
	destination port number in their packet headers. A port number is a 16-bit unsigned integer, ranging from 0 to 65535. A process associates its input or output channels via Internet sockets, a type of file descriptors, with a transport protocol, a port number and an IP address. This process is known as binding, which enables sending and receiving data via the network.
TLS	Transport Layer Security protocol that provides data secrecy and integrity between applications.
VoIP	Voice over Internet Protocol. Voice signals are transmitted over the Internet rather than over the public switched telephone network (PSTN).
VPN	Virtual Private Network extends a private network so that the resources that belong to that network are available by controlled remote access.
WebRTC	Web Real-Time Communication is an API definition drafted by the World Wide Web Consortium (W3C) to support browser-to-browser applications for voice, video chat, and P2P file sharing without either internal or external plug-ins.
WSS	Secure WebSocket protocol. Provides secure, full-duplex communication channels over a single TCP connection. Used in web browsers and web servers.

Reference Documents

Document Name	Link
Session Initiation Protocol	http://en.wikipedia.org/wiki/Session_Initiation_Protocol
RFC 3261 SIP: Session Initiation Protocol	http://www.ietf.org/rfc/rfc3261.txt
VoIP Reference Guide	http://www.voip-info.org/wiki/view/SIP
SIP Reference and Training	http://www.thesipschool.com/
WebRTC - Wikipedia	http://en.wikipedia.org/wiki/WebRTC