



The Intelligent Cloud Contact Center

Technical Requirements

Reference Guide

October 2026

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

Five9 and the Five9 logo are registered trademarks of Five9 and its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications, and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2026 Five9, Inc.

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

Five9®

Five9 Logo

Five9® SoCoCare™

Five9® Connect™

Contents

What's New	8
Environment and Security	11
RMI Protocol	11
RTP Protocol	11
Voice Quality Testing	12
Digital Certificates	12
DigiCert Certificates	13
Supported TLS Protocols	13
TLS Inbound Cipher Suites	14
TLS 1.3	14
TLS 1.2	14
TLS Outbound Cipher Suites	15
Setting the TLS Protocols in Your Browser	16
Web Browser Proxy Configuration	16
Five9 SIP Trunk Options	18
Private SIP Trunks Provided by Five9 ITSP Providers	18
SIP Trunks Provided by Your ITSP Provider	19
Private SIP Trunks for Five9 Gateway to Customer Gateway	19
Agent, Supervisor, and Administrator Applications	21
Requirements for Web-Based Applications	21
Workstation Requirements for Web-Based Applications	22
Hardware	22
Windows Platforms	22
Apple Mac Platforms	22
Chromebooks	22
Operating Systems	23
Windows 11 Efficiency Mode	23
Web Browsers	24
Windows Platforms	24
Apple Mac Platforms	24
Supported Voice Client Software Versions	24
Requirements for Five9 Video Engagement	25
Hardware	25
Windows Requirements	25
Apple Mac Requirements	25
Operating Systems	25
Web Browsers	26
Windows Platforms	26
Apple Mac Platforms	26
Mobile Devices	27
Video	27
Five9 Agent Assist Requirements	27

Virtual Desktop Requirements	28
Microsoft Multimedia Redirection for WebRTC	28
Amazon WorkSpaces Audio Redirection for WebRTC	28
Omnissa Horizon Audio Redirection for WebRTC	29
Citrix and VMware for Softphone and WebRTC	29
Options for Audio in Citrix/VMware	29
Audio Connections Outside the Virtual Channel on Citrix/VMware	30
Audio Connections Inside the Virtual Channel on Citrix/VMware	30
Softphone Audio Outside the Virtual Channel (Recommended on Citrix/VMware)	31
DVC Plug-In Mode and Fallback Support via Port 8083	31
PSTN and Gateway Mode Audio Outside the Virtual Channel	32
WebRTC or Softphone Audio Inside the Virtual Channel	32
Citrix/VMware Virtual Desktop Platforms	32
Citrix and VMware Supported Platforms	32
Supported Operating Systems in Citrix/VMware	32
Citrix/VMware Agent VDI Terminal Requirements	33
VDI View Clients	33
View Client Protocols	33
RDP View Protocol	34
Requirements for Java-Based Applications	34
Hardware	34
Windows Platforms	35
Apple Mac Platforms	35
Java Runtime Environment (JRE) for Applications	35
Operating Systems	36
Windows and Mac (32-bit and 64-Bit)	36
Windows 11 Efficiency Mode	36
Supervisor App for Apple iPad	37
Headset for Agents and Supervisors	37
Application Notes	38
Web Page Security and Visual IVR Scripts	38
Dashboards	38
Agent Desktop Plus with Digital Engagement	38
Integrated Administration Console	39
Five9 Agent Integrations	40
Requirements for Web-Based Adapters	40
Workstation Requirements for Web-Based Adapters	41
Hardware	41
Windows Platforms	41
Apple Mac Platforms	41
Operating Systems	41
Web Browsers	42

Five9 Fusion for Salesforce	42
Application Requirements	42
Plus Adapter for Agent Desktop Toolkit	42
Plus Adapter for Salesforce	43
Plus Adapter for Oracle Service Cloud	43
Plus Adapter for NetSuite	43
Plus Adapter for Microsoft Dynamics 365	43
Plus Adapter for Zendesk	44
Plus Adapter for ServiceNow	44
Plus Adapter for Epic	44
Five9 API Web Services (Custom Integration)	46
Verint Systems Requirements	47
Workstation Requirements	47
Hardware Requirements	48
Third-Party Software Required for Agent Stations	48
Third-Party Software Required for Browsing	49
Workstation Antivirus Settings	50
Java Runtime Settings Requirements for Verint	50
Supported Operating Systems	52
Supported Web Browsers	53
Microsoft Edge	53
Google Chrome	53
Chrome and Edge Considerations	54
Browser Requirements for Verint Player	54
Network Requirements (LAN and WAN)	55
Firewall Requirements	55
Studio Requirements	56
Studio Workstation Requirements	56
Studio Network Requirements	56
Determine Your Studio Environment	56
Studio 7 GCP-Hosted Network Requirements	57
Studio 7 CHI/VIR-Hosted Network Requirements	58
Public Internet Domains	58
Web Service Integration IP Addresses	58
Studio 7 CHI/VIR Migration to Google Cloud Platform (GCP)	58
Studio 6 Network Requirements	59
Public Internet Domains	59
Web Service Integration IP Addresses	59
SBC Public IP Addresses	61
RTP Proxy Public IP Addresses	62
Media Server Public IP Addresses	63

Network	65
Five9 Network Connectivity	65
Equinix Fabric	65
Agent Connect (MPLS)	66
Virtual Private Network (VPN)	66
VPN and Quality of Service (QOS)	66
VPN and Private IP Addresses	66
Direct Connect	67
Five9 Network Requirements (LAN and WAN)	67
Five9 Bandwidth Requirements	68
Five9 Network Recommendations	68
Bandwidth Requirements for Five9 Video Engagement for Agents	69
Other VoIP Services and Phones, Ports, IP Address Ranges, and Network Traffic	70
Five9 Internet Domains and IP Addresses	71
What Should I Include in my Allow List?	71
Five9 IP Address Ranges	72
Five9 IP Addresses for Identity Service Users	75
Five9 IP Addresses for Global Voice	75
Five9 IP Addresses for Email	76
Additional Five9 IP Addresses for Email	77
Five9 Connectivity Assessment Test	77
Five9 IP Addresses for Callback API Integration	78
Five9 IP Addresses for Professional Services Applications	78
Five9 IP Addresses for Verint Workforce Optimization	79
Verint IP Addresses for Global Voice	80
Five9 IP Addresses for VoiceStream	81
VoiceStream CTI Events and Webhooks	81
Five9 IP Addresses for Workflow Automation and Voice AI Agent	81
Five9 Addresses for Five9 University	82
Five9 Internet Domains	82
CounterPath Softphone Requirements	87
WebRTC Requirements	87
Performance Dashboard	88
SIP Firewall Note	90
TCP/UDP Port Requirements for Softphone Customers	91
TCP/UDP Port Requirements for WebRTC Customers	92
TCP/UDP Port Requirements for Gateway Customers	93
TCP/UDP Port Requirements for PSTN Customers	94
TCP and UDP Ports for Connectivity Assessment Test	94
TCP Port Requirements for FTP/SFTP	95
TCP Port Requirements for Five9 Performance Dashboard	95
Network Requirements for Five9 Video Engagement	95
Network Setup For Restricted Networks	96
Media Upload	96

SSL Interception	97
Monitoring Internet Bandwidth Usage	97
Implementing Quality of Service (QoS)	97
Port Requirements for Email	97
SOAP APIs	98
Third-Party Software	98
Five9 Quality of Service (QoS) Features	98
Workstation QoS Option	99
Network QoS Option	99
Application Usage Analytics	99
Workforce Engagement Management Requirements	100
Agent Workstation Requirements	100
Virtualized Agent Environments	100
Hardware Requirements	101
Operating Systems	101
Web Browsers	101
Software Requirements	102
Configuration Requirements	102
Firewall Policies	103
URLs	103
Supervisor Workstation Requirements	104
Virtualized Supervisor Environments	104
Hardware Requirements	104
Operating Systems	105
Web Browsers	105
Software Requirements	106
Configuration Requirements	106
Firewall Policies	106
Bandwidth Considerations	107
User Media Playback	107
Screen Capture Cache Transmission	107
Example Screen Capture Calculation	108
WEM IP Requirements	108
Reference Documents	109

What's New

Release	Change	Topic
Oct 2026	Added a section for IP address requirements for Professional Services applications.	Five9 IP Addresses for Professional Services Applications
Sep 2026	Added a note that to prevent dropped calls or one-way audio, network edge devices should send keep-alive traffic at an interval shorter than 30 seconds for any idle UDP connection.	Five9 Network Recommendations
	Updated requirements for agent applications and integrations to add support for macOS version 27 Golden Gate and to remove Windows 10.	Various
	Added support for WebRTC audio redirection on Omnisia Horizon.	Omnissia Horizon Audio Redirection for WebRTC
	Added support on Citrix and VMware for Windows 11 and Windows Server 2022 operating systems. Updated headings and descriptive text to clarify where requirements apply only to Citrix and VMware Horizon.	Citrix and VMware for Softphone and WebRTC
Aug 2026	Updated the list of required US domains with a missing URL supporting SOAP Configuration Web Services (api.five9.com). Updated the list of required India	Five9 Internet Domains

Release	Change	Topic
	domains with missing app server URLs (app.bom1.in.five9.com, app.del1.in.five9.com). Consolidated the list of shared domains that apply to each region.	
	Removed the Java-based Agent Desktop and Supervisor Desktop applications, which are no longer available as of August 1, 2026.	Requirements for Java-Based Applications
Jul 2026	Consolidated the IP requirements for Verint Workforce Optimization into a dedicated section, removing them from each region table. Updated the IP ranges for the US and India to provide subnets to support future expansion.	Five9 IP Addresses for Verint Workforce Optimization
	Added IP requirements for Five9 Global Voice for Verint Workforce Optimization customers.	Verint IP Addresses for Global Voice
	Updated the list of required domains with additional regional and data-center-specific variations for US, Canadian, and European data centers.	Five9 Internet Domains
Jun 2026	Updated IP requirements for callback API integrations to add new IP addresses and to remove obsolete ranges.	Five9 IP Addresses for Callback API Integration
	Updated IP requirements for email to add new IP addresses and to remove obsolete ranges.	Five9 IP Addresses for Email
	Added a new section for required IP ranges for Workflow Automation and AI Tools within Voice AI Agent.	Five9 IP Addresses for Workflow Automation and Voice AI Agent
	Corrected the London IP address for the Connectivity Assessment Test.	Five9 Connectivity Assessment Test

Release	Change	Topic
	Updated various IP range tables to remove duplication and to standardize formatting.	Five9 Internet Domains and IP Addresses
	Added support for the Australia release of ServiceNow and removed support for older versions. Removed support for the Classic workspace of ServiceNow.	Plus Adapter for ServiceNow
May 2026	Added a note that Five9 is ending support for Java-based Agent Desktop and Supervisor Desktop applications on August 1, 2026.	Requirements for Java-Based Applications
	Added a note that the Java Administrator app is not supported on Mac workstations using ARM processors.	Apple Mac Platforms
Mar 2026	Updated the network requirements for IVA Studio to clarify configurations for Studio 7 customers implemented on Google Cloud Platform (GCP) and on Five9 managed data centers (CHI/VIR).	Studio Network Requirements
	Updated IP requirements for callback API integrations to add new IP addresses and to remove obsolete ranges.	Five9 IP Addresses for Callback API Integration
	Updated IP requirements for email to add new IP addresses and to remove obsolete ranges.	Five9 IP Addresses for Email
	Added IP requirements for VoiceStream.	Five9 IP Addresses for VoiceStream

Environment and Security

The following sections describe environment and security requirements.

[RMI Protocol](#)
[RTP Protocol](#)
[Voice Quality Testing](#)
[Digital Certificates](#)
[Supported TLS Protocols](#)
[Web Browser Proxy Configuration](#)

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 (see [Enterprise-Ready Security](#)) 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 is 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, see [SSL Server Test](#).

TLS 1.3

Note: The suites shown below appear in a server-preferred order.

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2

Note: The suites shown below appear in a server-preferred order.

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CCM
- TLS_RSA_WITH_AES_128_CCM_8
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CCM
- TLS_RSA_WITH_AES_256_CCM_8
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

TLS Outbound Cipher Suites

The following are the supported TLS 1.2 outbound cipher suites. To verify that your servers support these ciphers, see [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 the TLS 1.2 encryption protocol in your browser security settings.

Important

For enhanced security, Five9 does not support inbound or outbound traffic using the TLS 1.1 protocol. Ensure that the TLS 1.2 protocol is enabled in your browser to connect to Five9 applications.

Web Browser Proxy Configuration

Port 8083 is required in the agents' workstations for the Five9 Softphone Service WebSocket TCP connection. Before you begin installing the softphone for agents on your network, complete the following configuration.

Important

If your network is set up to utilize local proxy settings for local traffic, you must create an exception for port 8083 before you install the softphone. Otherwise, the softphone connection will fail.

Do the following:

- 1 Enable WebSocket and localhost for port 8083.
- 2 Add this parameter to your proxy server: `ws://127.0.0.1:8083/*`

The syntax of the exception depends on your proxy server. For example, if you use Windows Group Policy to update your proxy server, update your Proxy Auto-Configuration (PAC) file with this parameter:

```
if (shExpMatch(url, "ws://127.0.0.1:8083/*")) {return "DIRECT";}
```

Ensure that localhost WebSocket traffic to port 8083 does not go through the proxy. In Windows LAN settings, depending on your configuration method for the proxy server, use either option:

- Automatic configuration: Ensure that your PAC file contains this exception:
`ws://127.0.0.1:8083/*`

- Manual configuration: Enable **Bypass proxy server for local address**.

When done, distribute your PAC file to all clients with your usual distribution method before you install the softphone.

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, or blended calls by Five9 Agents. SIP trunks support all domestic, International, and toll-free services.

[Private SIP Trunks Provided by Five9 ITSP Providers](#)

[SIP Trunks Provided by Your ITSP Provider](#)

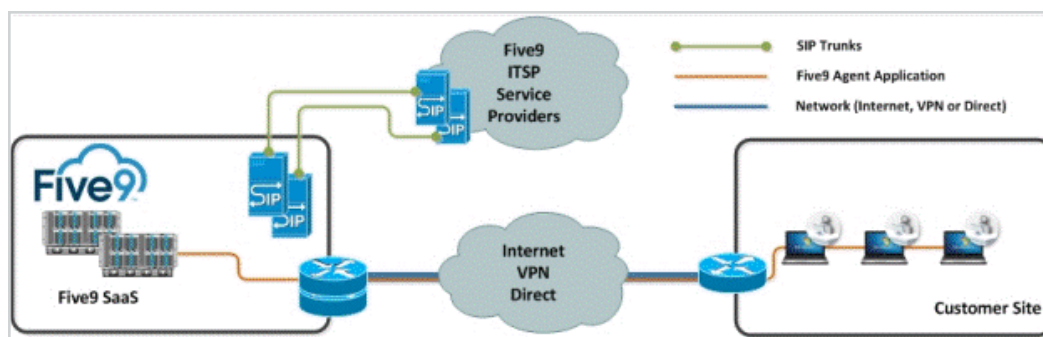
[Private SIP Trunks for Five9 Gateway to Customer Gateway](#)

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).

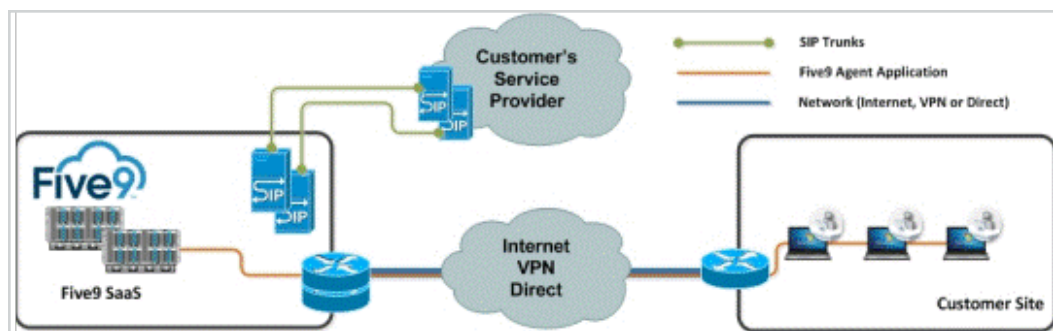
Private SIP Trunks Provided by Five9 ITSP Providers

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



SIP Trunks Provided by Your ITSP Provider

Your ITSP connects to the Five9 session border controllers (SBCs) in the Five9 data centers. To successfully configure, test, and turn up the SIP trunk, you must complete and return the installation checklist provided by your professional services implementation team. For more information, contact your Five9 representative.



Important

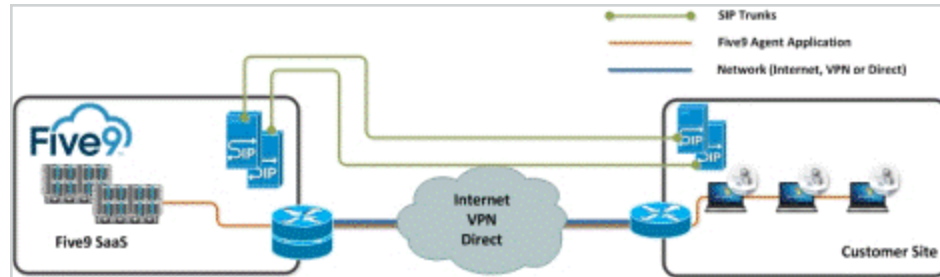
For details on integrating customer or vendor voice networks with Five9, see the [Five9 BYO SIP Trunk Integration Guide](#). Use the integration guide to confirm compatibility between voice edges and to review configuration details and requirements.

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 or through a VPN or Direct Connect Option.

Private SIP Trunks for Five9 Gateway to Customer Gateway



Agent, Supervisor, and Administrator Applications

The following sections describe agent, supervisor, and administrator application requirements.

[Requirements for Web-Based Applications](#)

[Five9 Agent Assist Requirements](#)

[Virtual Desktop Requirements](#)

[Requirements for Java-Based Applications](#)

[Headset for Agents and Supervisors](#)

[Application Notes](#)

Requirements for Web-Based Applications

These requirements apply to browser-based applications for agents, supervisors, and administrators, including Five9 Agent Assist, Agent Desktop Plus, Agent Desktop Toolkit, Supervisor Plus, Digital Engagement (SCC Admin), and Administrator Console.

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

[Workstation Requirements for Web-Based Applications](#)

[Requirements for Five9 Video Engagement](#)

Workstation Requirements for Web-Based Applications

Important

These requirements cover the use of Five9 applications. If agents use additional applications while using Five9 applications, be sure that each computer has sufficient hardware, a faster processor, and additional RAM to support all required applications.

If agents run multiple applications (tabs) in the browser in addition to Five9 applications, ensure that each computer has adequate RAM, or session disconnects could occur.

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
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 M3
Memory	8 GB	16 GB

Note: Five9 certifies software for Apple M3 (ARM64) processors.

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-Bit and 64-Bit	Windows 11 (all editions)
Apple macOS	Five9 supports the three most recent versions of macOS (excludes beta versions). • Version 15.0 Sequoia • Version 26.0 Tahoe • Version 27.0 Golden Gate
Chrome	Most recent three stable versions of Chrome.

Note

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 11 Efficiency Mode

Five9 recommends **turning off** Efficiency Mode on Windows 11 workstations used for live agent calls or for real-time customer service tasks.

Efficiency Mode reduces workstation power usage by limiting CPU resources for some foreground processes and by putting inactive browser tabs to sleep. These actions can interrupt Five9 applications in any supported browser and may cause issues such as **dropped active calls**.

Important: If you choose to keep Efficiency Mode on, configure agent workstations to use a **high-performance power plan**, such as the "Ultra Performance" power option on Dell workstations. Select a power plan profile that maintains peak performance and prevents the browser from placing inactive tabs into low-performance mode.

To confirm Efficiency Mode settings, open **Task Manager** and locate the Five9 process. Right-click the process. If **Efficiency mode** has a checkmark, it's enabled. To disable it, select Efficiency mode. The checkmark and status will be removed.

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-bit and 64-bit versions of the Chrome browser.
Firefox	Most recent three stable versions. Five9 supports 32-bit and 64-bit versions of the Firefox browser. ¹
Microsoft Edge	Most recent three stable versions. Five9 supports Microsoft Edge based on Chromium.
¹ Five9 does not recommend using Firefox for WebRTC when multiple tabs are used.	

Apple Mac Platforms

macOS 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.
Microsoft Edge	Most recent three stable versions. Five9 supports Microsoft Edge based on Chromium.

Supported Voice Client Software Versions

Five9 currently supports the following voice client software versions.

Voice Client Production/Version	Production
Softphone Installer	14.0.5
Softphone Chrome/Edge Extension	13.1.2 (recommended), 13.1.1
Softphone Firefox Extension	11.6.0

Requirements for Five9 Video Engagement

Hardware

Windows Requirements

Component	Minimum Version or Value	Recommended
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
Processor	- Intel Core i5, CPU 1.7 GHZ - Apple M1	- Intel Core i7, CPU 2.3 GHz - Apple M3
Memory	8 GB	16 GB

Note: Five9 certifies software for Apple M3 (ARM64) processors.

Operating Systems

Operating System	Version Supported
Windows 32-Bit and 64-Bit	Windows 11 (all editions)
Apple macOS	Five9 supports the three most recent versions of macOS (excludes beta versions).

Operating System	Version Supported
	• Version 15.0 Sequoia • Version 26.0 Tahoe • Version 27.0 Golden Gate

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-bit and 64-bit versions of the Chrome browser.
Firefox	Most recent three stable versions. Five9 supports 32-bit and 64-bit versions of the Firefox browser.
Microsoft Edge	Most recent three stable versions. Five9 supports Microsoft Edge based on Chromium.

Apple Mac Platforms

Browser	Version Supported
Google Chrome™	Most recent three stable versions. Google Chrome is automatically updated. Five9 supports 32-bit and 64-bit versions of the Chrome browser.
FireFox	Most recent three stable versions. Five9 supports 32-bit and 64-bit versions of the Firefox browser.
Microsoft Edge	Most recent three stable versions. Five9 supports Microsoft Edge based on Chromium.

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 and Android. For supported devices and for information on installing the SightCall app on mobile devices, see the SightCall documentation.

Video

To use Five9 Video Engagement, agents require a sound card and a built-in or standalone webcam. For information on requirements, see the SightCall documentation.

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. For the public IP list for LaunchDarkly, see 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.
pndsn.com	Access to messaging API (by PubNub) for client-side communication.

For Agent Assist bandwidth requirements, see [Five9 Bandwidth Requirements](#).

Virtual Desktop Requirements

These requirements provide guidance on the supported platforms and options for running Five9 applications in a virtual desktop infrastructure (VDI) environment. Agents and supervisors can access Five9 Plus applications from a virtual desktop to handle calls and process digital interactions (email, chat, and social).

For information about configuring and implementing VDI options, see the [Virtual Desktop Configuration Administrator's Guide](#).

Important

Five9 does not specify requirements or support for the virtualization server installation. For requirements and support information, contact your VDI vendor.

You are responsible for configuring, managing, and scaling your VDI environment to ensure optimal agent audio quality. Issues with audio must be reproducible in a non-VDI environment to be investigated by Five9.

Microsoft Multimedia Redirection for WebRTC

Microsoft Windows 365 Cloud PC and Azure Virtual Desktop officially support audio redirection from WebRTC utilizing the Microsoft Multimedia Redirection (MMR) toolkit. To access this toolkit, please contact your Microsoft account team.

Microsoft currently supports only Windows physical hardware for MMR.

For information on the requirements and configuration to use Five9 on Windows 365 Cloud PC and Azure Virtual Desktop, see [Windows 365 and Azure Virtual Desktop](#).

Amazon WorkSpaces Audio Redirection for WebRTC

Amazon WorkSpaces supports audio redirection in WebRTC. Five9 supports select versions of Linux, Windows 11, and Windows 10. Contact your Five9 account team to determine if your version of Linux is supported.

Important: Microsoft ended support for Windows 10 on October 14, 2025, and Five9 is no longer testing on that operating system. To avoid any potential service impacts, Five9 strongly recommends upgrading to Windows 11.

For information about the requirements and configuration to use Five9 on Amazon WorkSpaces, see [Amazon WorkSpaces](#).

Omnissa Horizon Audio Redirection for WebRTC

Omnissa Horizon supports audio redirection in WebRTC. Five9 supports select versions of Linux along with Windows 11 and Windows 10. Please contact your Five9 account team to determine if your version of Linux is supported.

Important: Microsoft ended support for Windows 10 on October 14, 2025, and Five9 is no longer testing on that operating system. To avoid any potential service impacts, Five9 strongly recommends upgrading to Windows 11.

For information about the requirements and configuration to use Five9 on Omnissa Horizon, see [Omnissa Horizon](#).

Citrix and VMware for Softphone and WebRTC

This section covers support for the following virtual desktop configurations:

- Citrix for softphone and WebRTC audio
- VMware Horizon for softphone audio only

Options for Audio in Citrix/VMware

There are two primary options for handling softphone or WebRTC call audio in a virtual desktop environment on Citrix or VMware.

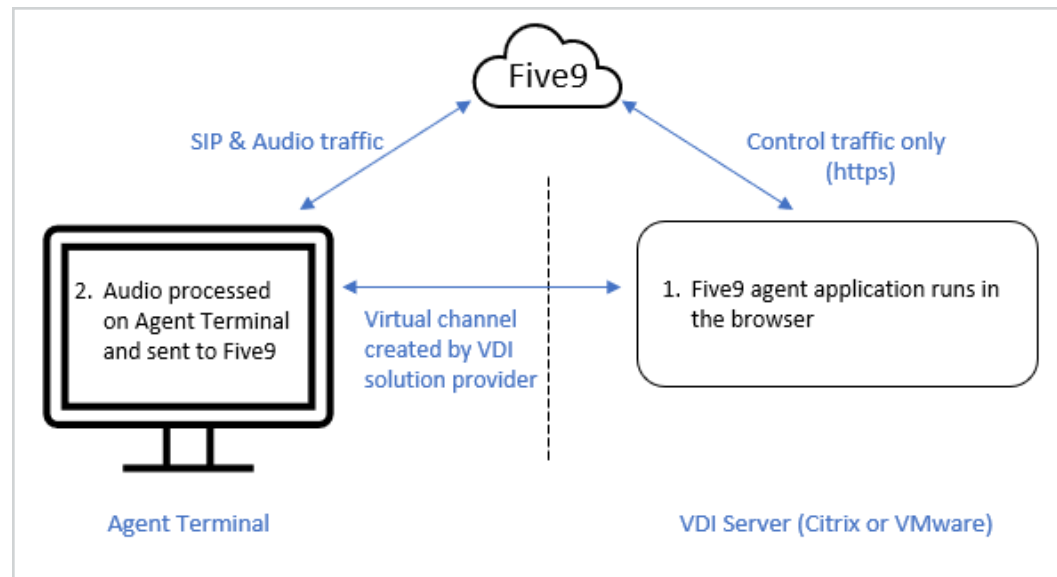
- Audio connections **outside** the virtual channel (recommended)
- Audio connections **inside** the virtual channel

Important

To ensure the best audio quality, Five9 recommends using options that process the audio outside the virtual session. Solutions that process the audio within the VDI session add a significant burden on shared VDI resources and are discouraged.

Audio Connections Outside the Virtual Channel on Citrix/VMware

Audio connections **outside** the virtual channel (recommended) support the softphone station type in VDI proxy mode.

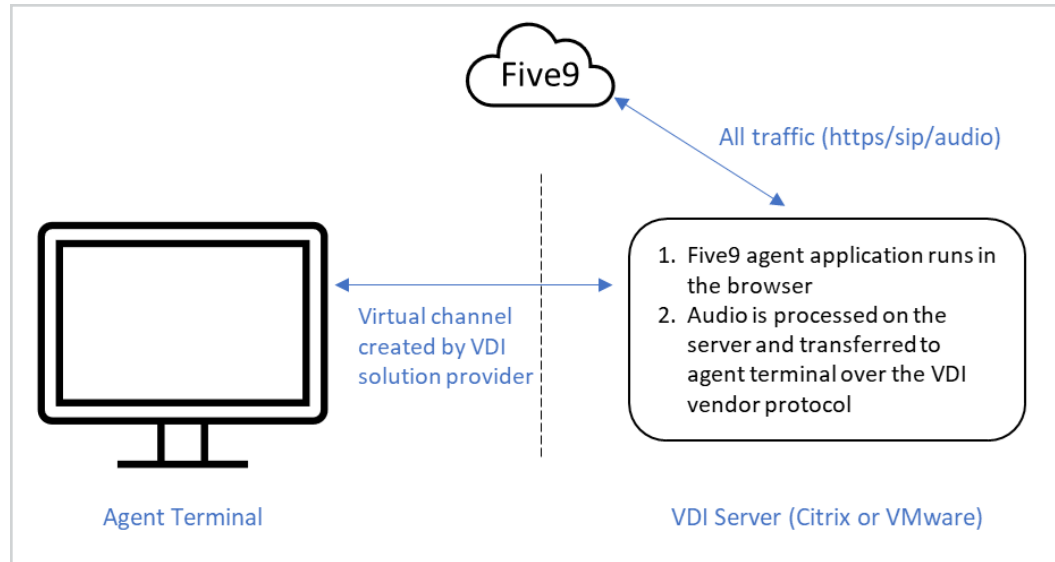


In this configuration, audio traffic is processed locally to the agent, while application data and control traffic are processed on the virtual desktop. When using the softphone in this mode, the softphone is installed on the agent terminal in *client mode* to process audio, and on the virtual desktop in *proxy mode* for call control functions.

Audio Connections Inside the Virtual Channel on Citrix/VMware

Audio connections **inside** the virtual channel support these station types:

- WebRTC
- Softphone in regular (non-VDI proxy) mode



In this configuration, applications, call audio, and call control run inside the virtual session. Five9 does not recommend this option because voice quality can suffer.

Softphone Audio Outside the Virtual Channel (Recommended on Citrix/VMware)

When audio runs outside the virtual channel, install the Five9 softphone service in *client* mode on the agent terminal and install the softphone in *proxy* mode on the virtual desktop to handle call control. The softphone audio is processed locally to the agent and voice traffic is between the agent terminal and Five9.

DVC Plug-In Mode and Fallback Support via Port 8083

The VDI proxy solution supports a Dynamic Virtual Channel (DVC) plug-in mode that enables the softphone in VDI proxy mode to support remote agents behind NAT firewalls or VPN.

The softphone in VDI proxy mode first attempts to connect using DVC. If that connection fails, it attempts to connect to the agent's terminal using port 8083. VPN is required between the VDI server and the agent's terminal in this case.

You must meet the following requirements to use the softphone in VDI proxy mode:

- Microsoft Windows is required on the agent terminal to use the DVC plug-in mode.
- Five9 supports macOS for agent terminals using the TCP port 8083 connection.

- Port 8083 must be open on the network and available between the virtual machine and the agent terminal.

Note

DVC plug-in mode does support the Citrix Virtual App with multi-session operating systems (formerly Citrix XenApp), but does not support a single-session operating system (formerly Citrix XenDesktop). The Five9 VDI solution with port 8083 supports both single-session and multi-session operating systems from Citrix.

PSTN and Gateway Mode Audio Outside the Virtual Channel

Five9 supports PSTN mode connections with telephony endpoints called over the PSTN or PBX endpoints over a private SIP trunk.

Five9 supports gateway mode connections with either a direct SIP station or a registered gateway SIP station with an external IP address.

Contact your Five9 representative to determine if these options are preferred options to the softphone in VDI proxy mode.

WebRTC or Softphone Audio Inside the Virtual Channel

For this setup, the agent terminal and VDI requirement are determined by the VDI solution and vendor you are using. Refer to your VDI vendor's website to understand agent terminal and VDI requirements.

Citrix/VMware Virtual Desktop Platforms

Five9 supports the following platforms and operating systems for virtualization on Citrix/VMware.

Citrix and VMware Supported Platforms

Five9 supports these platforms:

- Citrix Virtual Apps and Desktops version 1912 LTSR CU3
- Citrix Virtual Desktops version 7.15 LTSR CU8
- VMware Horizon version 7.13 CR

Supported Operating Systems in Citrix/VMware

Five9 supports these operating systems in virtual environments on Citrix/VMware:

- Microsoft Windows Desktop 10 and Windows Desktop 11
- Microsoft Windows Server 2019 and Windows Server 2022

Important: Microsoft ended support for Windows 10 on October 14, 2025, and Five9 is no longer testing on that operating system. To avoid any potential service impacts, Five9 strongly recommends upgrading to Windows 11.

Citrix/VMware Agent VDI Terminal Requirements

You may use Windows OS thin- or thick-clients with the softphone in VDI proxy mode. Five9 has tested these Windows thin clients:

- HP thin client t530/t540/t640
- Dell Wyse thin client 5079

Note

The Five9 softphone in VDI proxy mode and WebRTC do not support Zero clients.

Note

If you choose to run audio inside the virtual channel, WebRTC and the softphone can be supported on Linux OS thin clients. This option is not recommended for best audio quality.

VDI View Clients

Five9 supports the following view applications on the agent terminal device:

- Citrix Workspace 2019 (formerly Citrix Receiver). For detailed requirements, see [Citrix minimum requirements for Citrix Workspace](#).
- VMware Horizon Client 8.3.0. For detailed requirements, see [VMware minimum requirements for VMware Horizon Client, Windows](#).

Note

VMware Horizon Web Client is not supported.

View Client Protocols

Five9 supports these protocols:

- Citrix ICA and HDX
- VMware Blast and PCOIP

Note

The high-definition experience (HDX) protocol is supported when the softphone in VDI proxy mode is used in DVC plug-in mode. HDX protocol is not supported when using port 8083. For more information about HDX, see [How to Configure HDX Enlightened Data Transport Protocol](#)

RDP View Protocol

Five9 does not support RDP View protocol on VMware.

Requirements for Java-Based Applications

These requirements apply to the Java-based Five9 VCC Administrator application.

Important: The Java-based Agent Desktop and Supervisor Desktop applications are no longer available on the Five9 customer portal after August 1, 2026. Users must now use the browser-based Agent Desktop Plus and Supervisor Desktop Plus applications.

[Hardware](#)

[Java Runtime Environment \(JRE\) for Applications](#)

[Operating Systems](#)

[Supervisor App for Apple iPad](#)

Hardware

Important

These requirements cover the use of Five9 applications. If agents use additional applications while using Five9 applications, be sure that each computer has sufficient hardware, a faster processor, and additional RAM to support all required applications.

Important

If your domain has more than 5,000 users, ensure that any workstations that run the Java-based Administrator application meet the **recommended** hardware requirements (16GB RAM).

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
Memory	8 GB	16 GB
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.

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

Important

The Java-based VCC Administrator application is not supported on Mac workstations running ARM processors. To use the Java-based VCC Administrator on these workstations, use VCC Administrator via Web in Admin Console. For more information, see [VCC Administrator as a Web Application](#).

Java Runtime Environment (JRE) for Applications

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 VCC Administrator application will continue to work with Oracle Java SE. 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 421, 451, and 461.

Operating Systems

Windows and Mac (32-bit and 64-Bit)

Operating System	Version Supported
Windows 32-Bit and 64-Bit	Windows 11 (all editions)
Apple macOS	Five9 supports the three most recent versions of macOS (excludes beta versions). • Version 15.0 Sequoia • Version 26.0 Tahoe • Version 27.0 Golden Gate

Windows 11 Efficiency Mode

Five9 recommends **turning off** Efficiency Mode on Windows 11 workstations used for live agent calls or for real-time customer service tasks.

Efficiency Mode reduces workstation power usage by limiting CPU resources for some foreground processes and by putting inactive browser tabs to sleep. These actions can interrupt Five9 applications in any supported browser and may cause issues such as **dropped active calls**.

Important: If you choose to keep Efficiency Mode on, configure agent workstations to use a **high-performance power plan**, such as the "Ultra Performance" power option on Dell workstations. Select a power plan profile

that maintains peak performance and prevents the browser from placing inactive tabs into low-performance mode.

To confirm Efficiency Mode settings, open **Task Manager** and locate the Five9 process. Right-click the process. If **Efficiency mode** has a checkmark, it's enabled. To disable it, select Efficiency mode. The checkmark and status will be removed.

Supervisor App for Apple iPad

This section applies to the iPad Supervisor application. It does not apply to Supervisor Plus. The Java Supervisor client is no longer supported.

- Supported iPad models:
 - iPad Air
 - iPad mini 2 (Retina)
 - iPad 4
 - iPad mini
 - iPad 3
- Codecs: The primary codecs are G711U and G711A. You may also use GSM or ILBC, but these have not been tested.
- Browsers: Chrome is supported for the iPad Supervisor application.
- 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.

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](#)

[Dashboards](#)

[Agent Desktop Plus with Digital Engagement](#)

[Integrated Administration Console](#)

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, see

<http://erlend.oftedal.no/blog/tools/xframeoptions/>. For more information, see the [Interactive Voice Response \(IVR\) Administrator's Guide](#).

Browser	Version Supported	Version Partially Supported ²
Chrome		46, 47, 48, 54, 56, 67 52, 56 (Android phones)
Firefox	18 – 79	17
Opera		26
² 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

The following sections describe agent integration requirements.

[Requirements for Web-Based Adapters](#)
[Five9 API Web Services \(Custom Integration\)](#)

Requirements for Web-Based Adapters

These requirements apply to Five9 Plus adapters:

- Five9 Plus Adapter for Agent Desktop Toolkit
- Five9 Plus Adapter for Epic
- Five9Plus Adapter for Microsoft Dynamics 365
- Five9Plus Adapter for NetSuite
- Five9Plus Adapter for Oracle
- Five9Plus Adapter for Salesforce
- Five9 Plus Adapter for ServiceNow
- Five9Plus Adapter for Zendesk

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 for Web-Based Adapters](#)
[Application Requirements](#)

Workstation Requirements for Web-Based Adapters

Important

These requirements cover the use of Five9 adapters. If agents use additional applications while using Five9 applications, be sure that each computer has sufficient hardware, a faster processor, and additional RAM to support all required applications.

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
Memory	8 GB	16 GB
Screen Resolution	1024 x 768 or higher	1024 x 768 or higher

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 M3
Memory	8 GB	16 GB

Note: Five9 certifies software for Apple M3 (ARM64) processors.

Operating Systems

Operating System	Version Supported
Windows 32-Bit and 64-Bit	Windows 11 (all editions)
Apple macOS	Five9 supports the three most recent versions of macOS (excludes beta versions). - Version 15.0 Sequoia - Version 26.0 Tahoe - Version 27.0 Golden Gate

Web Browsers

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

Important

Five9 has ended support for Microsoft® Internet Explorer for all products. Five9 will continue to support Internet Explorer version 11 for the Oracle Service Cloud adapter only.

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-bit and 64-bit versions of the Chrome browser.	Windows and Mac
Firefox	Most recent three stable versions. Five9 supports 32-bit 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.	Windows and Mac

Five9 Fusion for Salesforce

Note: Salesforce Fusion is supported on Firefox and Chrome browsers.

Component	Minimum Version or Value
Processor	Intel Core i5-6500
Network	• 5 Mbps (minimum) • 10 Mbps (maximum)

Application Requirements

Plus Adapter for Agent Desktop Toolkit

No additional requirements.

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.

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

Important

Five9 is updating the Chrome extension to support Content Delivery Network (CDN) for the Plus Adapter for Netsuite. Ensure that you add the appropriate CDN domain to your firewall allowlist.

Data Center	Domain
US data centers	cdn.prod.us.five9.net
Canada data centers	cdn.prod.ca.five9.net
European data centers	cdn.prod.eu.five9.net
UK data centers	cdn.prod.uk.five9.net
India data centers	cdn.prod.in.five9.net

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.

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.

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 Service Operations and Configurable workspaces. It is compatible with the following ServiceNow releases:

- Australia
- Zurich
- Yokohama

Plus Adapter for Epic

Area	Requirements
Interface Support	• Epic Hyperdrive (Thin client, web-based) • Epic Hyperspace (Traditional client-based)
Deployment Models	• Epic Hosted (Epic-managed infrastructure) • Self-Hosted (Customer-managed infrastructure)
Supported Modules	• Compatible with most Epic modules. • Module-specific workspaces are available in Five9: ◦ Resolute – Revenue Cycle workspace ◦ Cadence – Scheduling workspace ◦ Other supported modules display their respective workspace dynamically within Five9. Note: The Willow (Rx) module is not supported.
Virtualization Support	Compatible with launching Epic through Citrix. Additional implementation effort may be required for Citrix-based deployments.
Epic Version Compatibility	Fully supports Epic May 2024 release and all later versions.
Architecture and Cost	Epic Adapter v1.0 is built using Epic's free APIs.

Area	Requirements
Considerations	Note: No additional Epic data dip charges incur when using this adapter.

Five9 API Web Services (Custom Integration)

The Five9 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.

For information on each API and its limitations, refer to the appropriate documentation. These are primary resources:

- The [Agent and Supervisor REST APIs Developer's Guide](#) describes methods for accessing and managing the Five9 Cloud Contact Center.
- The [Five9 CRM SDK JavaScript library](#) provides APIs for interaction with the Plus Adapter for Agent Desktop Toolkit.

Additional API guides are found on the [Developer PDFs](#) page on the Five9 documentation website.

Verint Systems Requirements

Verint Systems® is a browser-based application that provides agent analytics and performance evaluation. The following sections describe requirements for Verint Systems.

[Workstation Requirements](#)
[Network Requirements \(LAN and WAN\)](#)

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](#)
[Third-Party Software Required for Agent Stations](#)
[Third-Party Software Required for Browsing](#)
[Workstation Antivirus Settings](#)
[Java Runtime Settings Requirements for Verint](#)
[Supported Operating Systems](#)
[Supported Web Browsers](#)
[Browser Requirements for Verint Player](#)

Hardware Requirements

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

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.

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, both 32-bit and 64-bit redistributables must be installed.

Desktop Application	Required Third-Party Software
DPA Validator	- Microsoft .NET Framework 4.6.2 and higher versions supported by Microsoft on the Windows operating system. - Microsoft Visual C++ 2015 Redistributable or higher 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	Microsoft Windows Installer 5.0 or later.
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.
Screen Capture Module	- Microsoft Windows Installer 2.0 or later. - Microsoft Visual C++ 2019 Redistributable 32-bit. - Microsoft .NET Framework 4.6.2 or 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 - Verify that the JAVA_HOME environment variable is set to 32-bit installation of Java.

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	The Strategic Planner web desktop application requires JRE.

Software	Web-Based Application
approved minor version releases.	
Windows Media Player 12	Required to play files from workstations without browsing to the Interactions Home Page.

Workstation Antivirus Settings

When workstations use real-time antivirus scans, there are file extensions, files, and folders in the Verint application that should not be scanned by antivirus applications.

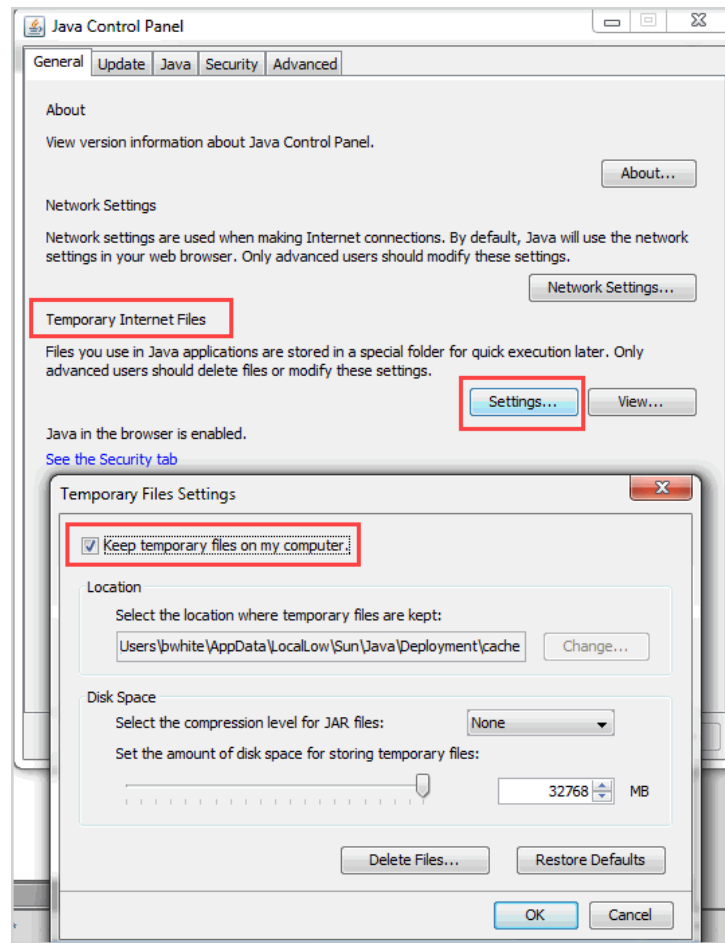
To prevent scanning these files, ensure that each workstation is set up to exclude the following items.

Default Folder	Exclusion List
%PROGRAMFILES%\Verint\DPA\Client	Exclude all files and subfolders, or the process DCUApp.exe.
%PROGRAMDATA%\Verint\DPA\Data	Exclude all files and subfolders, or the process DCUApp.exe. Exclude the following typical file extensions at a minimum: *.svn, *.htm, *.sxn, *.ini, *.def, *.pds, *.xml, *.bmp, *.txt.
CaptureService\Screen Capture Module	Exclude all files and subfolders, or the process CaptureService.exe.

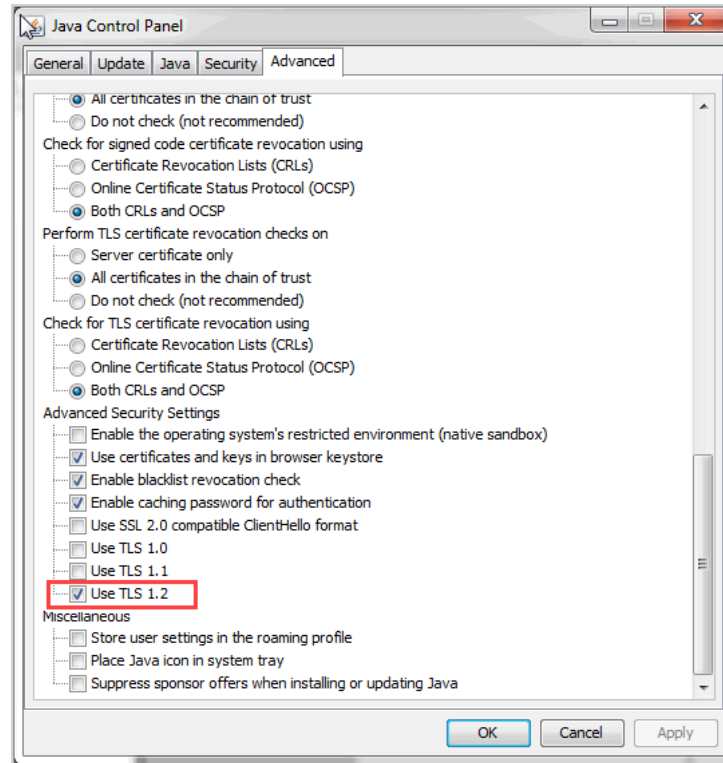
Java Runtime Settings Requirements for Verint

Verify the following Java Runtime Environment (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 1.2**.



Supported Operating Systems

Operating System	Version Supported
Microsoft Windows 10 Pro and Enterprise	32-bit and 64-bit
Microsoft Windows 11 Pro and Enterprise	
Microsoft Windows Server 2022 (with Desktop Experience) Standard and Datacenter editions	
Microsoft Windows Server 2019 (with Desktop Experience) Standard and Datacenter editions	
Microsoft Windows Server 2016 (with Desktop Experience) Standard and Datacenter editions	

Important: Microsoft ended support for Windows 10 on October 14, 2025, and Five9 is no longer testing on that operating system. To avoid any potential service impacts, Five9 strongly recommends upgrading to Windows 11.

Supported Web Browsers

Microsoft Edge

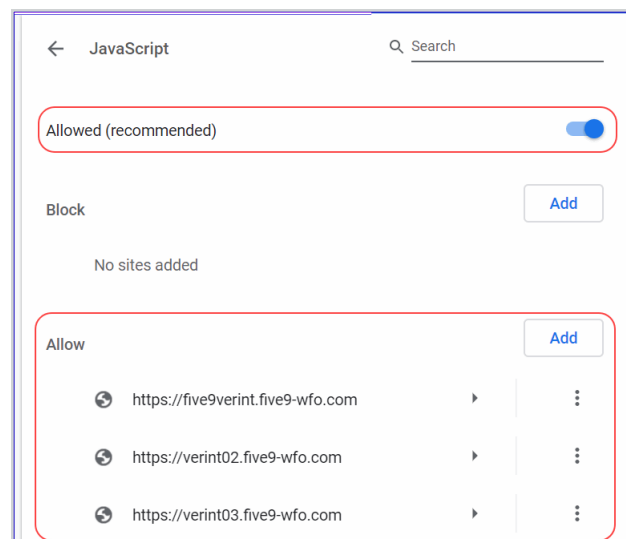
Microsoft® Edge for Chromium v125 or higher is supported.

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



- 2 To add the five9-wfo portal addresses to the list of sites allowed to run JavaScript, click **Add**. For a list of addresses, see [Five9 IP Address Ranges](#).

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

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

- 3 To enable pop-ups, select **Pop-ups Allowed** and add the **five9-wfo** sites to the list of sites allowed to display pop-ups.
- 4 To allow file downloads from the portal, such as DPA validator and reports, select **Ask** or **Allow** for automatic downloads.



Chrome and Edge Considerations

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

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

- 1 Third Party Software Required for Agent Stations for Verint
 - a In the Logger row, update to Microsoft .NET Framework 4.6.2 or 4.7.x, or 4.8.x

Browser Requirements for Verint Player

Google® streaming media player is the default player when working in Google Chrome or Microsoft® Edge for Chromium.

Interaction playback in Chrome or Edge for Chromium streams playback and does not require installation of the Plugin Playback on the user's desktop. The streaming player uses the native browser capabilities to perform playback.

Network Requirements (LAN and WAN)

If you use Screen Recording, an additional 160kbps is required for each agent in addition to the stated bandwidth requirements.

For a full list of bandwidth requirements, see [Five9 Network Requirements \(LAN and WAN\)](#).

Firewall Requirements

These ports must be open for Verint application features. These ports apply to US, Canada, 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)
29434	TCP	Outbound	Verint Systems Cloud Screen Recorder
29436	TCP	Outbound	Verint Systems RIS servers

Studio Requirements

Five9 Studio is an omnichannel cloud-based platform used to deploy Intelligent Virtual Agents (IVAs) and self-service applications.

The following sections describe requirements for Studio.

Studio Workstation Requirements

Studio developers work in a browser application to design Intelligent Virtual Agent applications. Studio supports these configurations:

- **Operating System:** Latest Windows and macOS versions.
- **Browser:** Google Chrome only.

Studio Network Requirements

Five9 IVA Studio customers must use these requirements to configure network allow lists for full connectivity.

Determine Your Studio Environment

Studio network requirements fall into three major categories depending on the version and location of Studio. To determine your IVA Studio version, log in to IVA Studio design time and check the browser URL bar. Use the categories below to determine your requirements, or contact your Five9 representative.

Studio 7 – Google Cloud Platform (GCP) Hosted: All Five9 Studio customers implemented after January 2026 are in Studio 7 GCP-hosted environments. Representative URLs are:

- <https://us-01.studio.us.five9.net>
- <https://us-02.studio.us.five9.net>
- <https://us-03.studio.us.five9.net>
- <https://us-04.studio.us.five9.net>
- <https://studio.eu.five9.net>
- <https://studio.uk.five9.net>

Studio 7 – CHI/VIR Hosted: Customers implemented before January 2026 who log in through <https://admin.us.five9.net> to access Studio are hosted in the CHI/VIR data centers. The Studio portal URL is <https://five9.us7.studiportal.io>.

Studio 6: Customers on Studio 6 use the following log in portals:

- US Studio 6 Colo: <https://usstudio.inferencecommunications.com>,
<https://five9.us.studiportal.io>
- UK Studio 6: <https://ukstudio.inferencecommunications.com>,
<https://five9.au.studiportal.io>
- Canada Studio 6: <https://castudio.inferencecommunications.com>,
<https://five9.ca.studiportal.io>
- Australia Studio 6: <https://ausstudio.inferencecommunications.com>,
<https://five9.uk.studiportal.io>
- Brazil Studio 6: <https://brstudio.inferencecommunications.com>,
<https://five9.br.studiportal.io>

Studio 7 GCP-Hosted Network Requirements

IVA Studio customers implemented on GCP must follow the network requirements for IP addresses and domains that apply to the full Five9 platform and services.

Use the configurations in [Five9 Internet Domains and IP Addresses](#) rather than the configurations on this page.

Studio 7 CHI/VIR-Hosted Network Requirements

Public Internet Domains

This table lists the URL to access the Studio Portal.

URL	Location	Services
https://five9.us7.studioportal.io	US, South America	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 by Five9 on studioportal.io subdomains use the following IP addresses. For services accessed by five9.net subdomains, refer to addresses detailed in [Five9 IP Addresses for Callback API Integration](#).

USA Integration IPs.

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

Studio 7 CHI/VIR Migration to Google Cloud Platform (GCP)

For improved scale and reliability, Five9 is adding the ability for traffic for all Studio 7 customers to be served out of the Five9 GCP tenant in addition to the CHI/VIR managed data centers.

Beginning in March 2026, traffic originating from Five9 IVA Studio, such as integrations into third party APIs or systems, may observe different source IP ranges than before. Additionally, API requests made to Studio 7 APIs may resolve to alternative IP ranges.

Important

All customers on Studio 7 in the US **must** allow the IP addresses that support the Five9 US presence. Ensure that the set of IP ranges in the table at [US IP Ranges](#) are opened on your firewall.

If you are using API Integration node callbacks, make sure you allow the US IP ranges in the table at [Five9 IP Addresses for Callback API Integration](#).

Studio 6 Network Requirements

Public Internet Domains

This table lists the URLs to access the Studio Portal.

URLs	Location	Services
https://five9.us.studioportal.io https://usstudio.inferencecommunications.com	US, South America	Studio Portal, Studio API
https://five9.au.studioportal.io https://ausstudio.inferencecommunications.com	Australia, New Zealand, Japan, Southeast Asia	Studio Portal, Studio API
https://five9.ca.studioportal.io https://castudio.inferencecommunications.com	Canada	Studio Portal, Studio API
https://five9.uk.studioportal.io https://ukstudio.inferencecommunications.com	EU, UK, Africa	Studio Portal, Studio API
https://five9.br.studioportal.io https://brstudio.inferencecommunications.com	Brazil	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 such 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	Tertiary AZ
35.182.62.129	35.183.166.219	52.60.47.143

Brazil Sao Paulo IPs.

Primary AZ	Secondary AZ
18.231.3.237	177.71.160.47
	54.232.173.97 (alternate)

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 wanting 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)
primary.sip.us.inferencecommunications.com 199.189.191.98	secondary.sip.us.inferencecommunications.com 208.71.166.115
Virginia PCI (Primary Site)	Chicago PCI (Secondary Site)
primary.sip.pci.us.inferencecommunications.com 199.19.68.222	secondary.sip.pci.us.inferencecommunications.com 208.71.166.109

Australia SBC IPs.

Melbourne (Primary Site)	Sydney (Secondary Site)
primary.sip.au.inferencecommunications.com 202.147.130.82	secondary.sip.au.inferencecommunications.com 202.147.130.90
Melbourne PCI (Primary Site)	Sydney PCI (Secondary Site)
primary.sip.pci.au.inferencecommunications.com 202.147.129.156	secondary.sip.pci.au.inferencecommunications.com 202.147.130.93

UK SBC IPs.

Primary AZ	Secondary AZ
primary.sip.uk.inferencecommunications.com 34.255.92.105	secondary.sip.uk.inferencecommunications.com 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

Brazil SBC IPs.

Primary AZ	Secondary AZ
primary.sip.br.inferencecommunications.com 18.229.4.210	secondary.sip.br.inferencecommunications.com 54.233.181.175

RTP Proxy Public IP Addresses

Region	Public IP Address	Port Range
Virginia non-PCI	199.189.191.77 199.189.191.78 199.189.191.98	35000 - 65000
Virginia PCI	199.19.68.222	35000 - 65000
Chicago non-PCI	208.71.166.113 208.71.166.114 208.71.166.115	35000 - 65000
Chicago PCI	208.71.166.109	35000 - 65000
Melbourne non-PCI	202.147.130.82	35000 - 65000
Melbourne PCI	202.147.129.156	35000 - 65000
Sydney non-PCI	202.147.130.90	35000 - 65000
Sydney PCI	202.147.130.93	35000 - 65000
UK	52.18.167.135, 34.246.159.75	35000 - 65000

Region	Public IP Address	Port Range
Canada	99.79.92.109, 52.60.164.146	35000 - 65000
Brazil	18.228.141.173, 18.228.158.129	35000 - 65000

Media Server Public IP Addresses

USA Virginia Media Server Public IPs.

IP Addresses
104.37.106.48/28
199.19.68.208/28
199.189.191.64/28

USA Chicago Media Server Public IPs.

IP Address
199.189.190.64/28
199.189.190.96/28
208.71.166.96/28

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

Brazil Media Proxy IPs.

Primary	Secondary
18.228.158.129	18.228.141.173

Network

The following sections describe network and connectivity requirements

[Five9 Network Connectivity](#)

[Five9 Network Requirements \(LAN and WAN\)](#)

[Other VoIP Services and Phones, Ports, IP Address Ranges, and Network Traffic](#)

Five9 Network Connectivity

There are multiple Wide Area Network (WAN) options available to connect directly and securely into the Five9 data centers. Depending on the option that you select, you may have to install networking equipment such as a router or firewall within the Five9 data center.

The following connectivity options are available.

[Equinix Fabric](#)

[Agent Connect \(MPLS\)](#)

[Virtual Private Network \(VPN\)](#)

[Direct Connect](#)

Equinix Fabric

Five9 has partnered with Equinix to leverage the power of their Fabric to enable you to establish secure dedicated bandwidth connections to Five9.

The Equinix Fabric™ is for customers who have networking equipment in Equinix Fabric™ enabled co-locations. You procure Layer-2, Equinix Fabric connectors directly from Equinix, who provides the Service Level Agreements (SLAs) for latency, packet loss, and jitter when connecting to Five9 Edge locations.

Equinix Fabric is supported in the Five9 Edge locations:

- Chicago, US (CH3)
- Washington D.C., US (DC10)
- London, UK (LD5)

- Amsterdam, NL (AM4)
- Frankfurt, DE (FR8)
- Sao Paulo, BR (SP4)
- Tokyo, JP (TY11)
- Sydney, AU (SY5)

Agent Connect (MPLS)

You may procure MPLS services from Five9.

For more information about this connectivity option, contact your Five9 account manager.

Virtual Private Network (VPN)

Five9 offers a VPN option for direct connection to the Five9 data centers, for secure encrypted transmission of voice and data transmission over the internet. Five9 can support a site-to-site connection to any industry-standard VPN solution.

Customers with split-tunnel VPN configurations should not exclude Five9 domains from their VPN. Doing so ensures consistent DNS resolution, regardless of whether the VPN is active.

For VPN bandwidth requirements, see [Five9 Bandwidth Requirements](#).

VPN and Quality of Service (QoS)

IP connections, such as Agent Connect (MPLS), Equinix Fabric™, or Direct Connect, 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

Generally, VPN is used 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 Connect

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 your network and Five9 network provides enough bandwidth. The limiting factor is usually the last mile connection to your premises. If you are required to establish direct connection to a Five9 data center, such as through MPLS or Equinix Fabric™, the Direct Connect option provides this capability.

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

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 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).

For more information about these connection options, contact your Five9 account manager.

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 - 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
Five9 UC - Nextiva	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

Connection Type	Support Details
	subject to higher latency, which can affect the Quality of Service (QoS).
Wireless LANs (Wi-Fi)	Five9 recommends wired connections for best results, however wireless Local Area Networks (LANs) are supported as long as each user can meet the minimum bandwidth requirements for softphone/WebRTC calls (see Five9 Bandwidth Requirements).
Satellite and Wireless Internet	Satellite and wireless Internet connections are not supported, for example, 5G and cellular.
SIP and RTP Traffic	Do not restrict SIP and RTP traffic across LANs or WANs when multiple customer sites exist.
NAT and PAT	NAT and PAT are supported configurations. Double Network Address Translation (Double NAT) is not supported.

Note: The Five9 NAT gateway has a 30-second idle timeout for UDP sessions (SIP signaling and RTP media). To prevent dropped calls or one-way audio, ensure your firewall, SBC, or NAT device sends keep-alive traffic (or maintains its own NAT binding) at an interval shorter than 30 seconds for any idle connection.

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	30 Kbps	130 Kbps	130 Kbps	130 Kbps
Conference Additional Passive Speaker*	0 Kbps	+40 Kbps	+40 Kbps	+40 Kbps
<i>*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.</i>				
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:443. The default port is generally omitted. Five9 URLs do not use a port other than 443.

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](#)
[SIP Firewall Note](#)
[TCP/UDP Port Requirements for Softphone Customers](#)
[TCP/UDP Port Requirements for WebRTC Customers](#)
[TCP/UDP Port Requirements for Gateway Customers](#)
[TCP/UDP Port Requirements for PSTN Customers](#)
[TCP and UDP Ports for Connectivity Assessment Test](#)
[TCP Port Requirements for FTP/SFTP](#)
[TCP Port Requirements for Five9 Performance Dashboard](#)
[Network Requirements for Five9 Video Engagement](#)
[Port Requirements for Email](#)
[SOAP APIs](#)
[Third-Party Software](#)
[Five9 Quality of Service \(QoS\) Features](#)
[Application Usage Analytics](#)

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 (your allow list). 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.

Important

Five9 uses a two-minute TTL (time-to-live) setting on DNS records used for automated failover between primary and secondary sites. Ensure that DNS caching on your network does not override this two-minute TTL to avoid potential issues in the event of a failover.

What Should I Include in my Allow List?

This section outlines how to use the provided information to add the specified IP addresses to your allow list.

- Determine your allow list. Including IP addresses on an allow list allows certain IP addresses or ranges to access or engage with systems or services.
- Include the specified IP address ranges from the [Five9 IP Address Ranges](#). These must be included. In addition to these IP ranges, add the IPs provided in the subsections in this section depending on additional services.

Note

For information on network requirements for IVA Studio 6 or IVA Studio 7 hosted on the CHI/VIR managed data centers, see [Studio Network Requirements](#).

Five9 IP Address Ranges

To avoid potential service impacts, all of the following Five9 IP addresses **must** be added to a list of allowed entities in your IPS solutions. In addition to these IP ranges, add the IPs provided in the subsections in this section depending on additional services.

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.

Note

For IP addresses required for Verint Workforce Optimization, see [Five9 IP Addresses for Verint Workforce Optimization](#).

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
35.241.29.181	login.auth.five9.com	
	migrate.auth.five9.com	
https://s3.amazonaws.com/okta-ip-ranges/ip-ranges.json	auth.five9.com	

Note: IPs listed in `us_cell_12` in the

US IP Ranges	Location of Data Center	CIDR Format
above link.		

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	Canada data center	74.114.192.0/23
34.95.54.0 – 34.95.54.63		34.95.54.0/26
147.124.160.0 – 147.124.191.255		147.124.160.0/19
35.203.118.198		35.203.118.198/32
34.95.20.197	login.five9.ca	
35.203.62.218		
34.95.47.32	api.five9.ca	
35.203.0.33		
35.203.103.232	app.ca.five9.com	
34.95.57.4		
35.203.103.118	ca1.ca.five9.com	
35.203.54.96	ca2.ca.five9.com	
34.160.54.11	login.auth.ca.five9.com migrate.auth.ca.five9.com	
https://s3.amazonaws.com/okta-ip-ranges/ip_ranges.json	auth.ca.five9.com	

Note: IPs listed in **us_cell_14** in the above line.

In Canada, other data centers are optional.

EU/UK IP Ranges	Location of Data Center	CIDR Format
185.111.40.0 – 185.111.40.255	London	185.111.40.0/24
185.111.43.0 – 185.111.43.255		185.111.43.0/24
212.187.211.0 – 212.187.211.255		212.187.211.0/24
147.189.16.0 – 147.189.31.255		147.189.16.0/20
147.189.224.0 – 147.189.239.255		147.189.224.0/20

EU/UK IP Ranges	Location of Data Center	CIDR Format
147.189.239.128 – 147.189.239.191		147.189.239.128/26
147.189.239.192 – 147.189.239.207		147.189.239.192/28
34.89.67.64 - 34.89.67.127	London GCP	34.89.67.64/26
34.160.81.177	login.auth.five9.eu (UK) migrate.auth.five9.eu (UK)	
https://s3.amazonaws.com/okta-ip-ranges/ip_ranges.json	auth.five9.eu (UK)	
Note: IPs listed in emea_cell_2 in the above link.		
185.111.42.0 – 185.111.42.255	Amsterdam Network Edge	185.111.42.0/24
185.111.41.0 – 185.111.41.255	Frankfurt Network Edge	185.111.41.0/24
34.117.237.99	login.auth.eu.five9.com (EU) migrate.auth.eu.five9.com (EU)	
https://s3.amazonaws.com/okta-ip-ranges/ip-ranges.json	auth.eu.five9.com (EU)	
Note: IPs listed in emea_cell_2 in the above link.		
147.189.239.0 – 147.189.239.63	Frankfurt GCP	147.189.239.0/26
147.189.239.224		147.189.239.224/28
147.189.239.64 – 147.189.239.127	Netherlands GCP	147.189.239.64/26
147.189.239.240		147.189.239.240/28
<i>The EU and UK data centers have some shared resources for redundancy. Other data centers are optional.</i>		

India IP Ranges	Location of Data Center	CIDR Format
202.92.194.0 – 202.92.194.255	India Telephony Edge Mumbai (BOM)	202.92.194.0/24
202.92.195.0 – 202.92.195.255	India Telephony Edge Delhi (DEL)	202.92.195.0/24
202.92.197.0 – 202.92.197.255	India WFO (AWS)	202.92.197.0/24
202.92.198.0 – 202.92.198.255	India GCP	202.92.198.0/24
202.92.199.0 – 202.92.199.255		202.92.199.0/24

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 Identity Service Users

The IP addresses listed below are exclusively for Five9 Identity Service. Ensure that you add the Amazon Web Services IP address ranges for your region. These addresses are in addition to the [Five9 IP Address Ranges](#).

Data Center	IP Address Range	Domain	Additional Information
US	https://s3.amazonaws.com/okta-ip-ranges/ip_ranges.json	auth.five9.com	IPs listed in us_cell_12
Canada	https://s3.amazonaws.com/okta-ip-ranges/ip_ranges.json	auth.ca.five9.com	IPs listed in us_cell_14
UK	https://s3.amazonaws.com/okta-ip-ranges/ip_ranges.json	auth.eu.five9.com	IPs listed in emea_cell_2
EU	https://s3.amazonaws.com/okta-ip-ranges/ip_ranges.json	auth.five9.eu	IPs listed in emea_cell_2

Five9 IP Addresses for Global Voice

The IP addresses listed below are exclusively for Five9 Global Voice (FGV). These addresses are in addition to the [Five9 IP Address Ranges](#).

Important

Five9 is expanding Global Voice for Dublin with new IP address ranges. To avoid any potential service impact, Five9 strongly recommends that you add both **185.111.43.0/24** and **212.187.211.0/24** to your firewall IP allow list by September 25, 2024. **Do not** remove the current IP address from your existing IP allow list.

Location	IP Address
Dublin	34.241.191.251 185.111.43.0/24 212.187.211.0/24
Sao Paulo	209.14.129.0/24
Sydney	103.169.229.0/24
Tokyo	103.169.228.0/24

Five9 IP Addresses for Email

The IP addresses listed below are exclusively for Five9 IP Addresses for Email. These addresses are in addition to the [Five9 IP Address Ranges](#).

Note

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

Location of Data Center	IP Addresses
US	147.124.171.128/28 147.124.191.0/28 147.124.171.192/28 147.124.191.208/28 147.124.171.160/28 198.105.204.18 198.105.204.19 198.105.204.20 198.105.205.18 198.105.205.19 198.105.205.20
CA	147.124.171.224/28 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
UK	147.189.239.208/28

Location of Data Center	IP Addresses
	185.49.234.25
	185.49.234.29
	185.49.234.30
EU	147.189.238.128/28
IN	202.92.198.144/28

Additional Five9 IP Addresses for Email

If you use Five9 for email interactions and restrict traffic through your firewall, you must use one of the following methods to add this required entity to your allow list. These addresses are in addition to the [Five9 IP Address Ranges](#).

- Add the **storage.googleapis.com** domain
- Run **host storage.googleapis.com** and add the generated IP addresses

Note: Google may change the list of IP addresses for this resource over time without notice. If so, you will need to update the allow list.

Five9 Connectivity Assessment Test

The IP addresses listed below are exclusively for Five9 Connectivity Assessment Test. These addresses are in addition to the [Five9 IP Address Ranges](#).

Location	IP Address
Santa Clara	38.107.71.103
Santa Clara	198.105.200.22 - 198.105.200.25
Atlanta	198.105.202.16 - 198.105.202.18, 198.105.202.9
London	212.187.211.5 - 212.187.211.6
Canada	35.203.75.94
Tokyo	52.196.118.63
Sydney	3.105.227.19
Sao Paulo	18.229.56.203
Dublin	108.129.62.47

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 firewall allow list. These addresses are in addition to the [Five9 IP Address Ranges](#).

Location	IP Address
US	147.124.171.128/28
	147.124.171.192/28
	147.124.191.0/28
	147.124.191.208/28
	147.124.171.160/28
CA	147.124.171.224/28
EU	147.189.238.128/28
UK	147.189.239.208/28
IN	202.92.198.144/28

Five9 IP Addresses for Professional Services Applications

The IP addresses listed below are exclusively for Five9 Professional Services applications. Add the IP addresses for the Professional Services applications you use to your firewall allow list. These addresses are required in addition to the [Five9 IP Address Ranges](#).

Note

- If you use a Five9 PS proxy, allow the Proxy Services IP addresses. PS proxies can include SOAP Proxy and Mutual Auth Proxy. If you are unsure whether your integration is a PS proxy, confirm with your assigned Five9 Deployment Resource.
- If your solution is a bespoke Custom Solution, or an application not listed below, contact your assigned Five9 Deployment Resource to confirm if any IP addresses apply.

Location	Application	IP Address
US	Automated Messaging	35.239.11.98
	Cacher	34.10.230.175, 34.69.219.148, 34.71.196.45, 34.122.34.12, 35.202.230.168, 35.225.113.27, 35.239.61.221, 136.114.141.254
	LiveChat Add-on	35.225.113.27, 35.239.61.221
	Proxy Services	34.10.230.175, 34.69.219.148, 34.71.196.45, 34.122.34.12, 35.202.230.168, 35.225.113.27, 35.239.61.221, 136.114.141.254
	PS SMS	34.134.60.27, 35.225.113.27, 35.239.61.221, 104.154.239.72
	Social Messaging Service	34.134.60.27, 104.154.239.72
	Transcribe	34.10.230.175, 34.69.219.148, 34.71.196.45, 34.122.34.12, 35.202.230.168, 35.225.113.27, 35.239.61.221, 136.114.141.254
	Verint Data Manager	34.10.206.199, 34.66.228.10, 34.171.99.211
Canada	PS SMS	34.118.156.226, 35.203.64.88
	Social Messaging Service	34.118.156.226
EU	Cacher	34.12.51.217, 34.12.164.52
UK	Automated Messaging	35.246.71.203
	Proxy Services	34.89.3.98, 35.189.69.1
	PS SMS	34.147.221.98, 35.246.53.148
	Social Messaging Service	34.147.221.98

Five9 IP Addresses for Verint Workforce Optimization

The IP addresses listed below are exclusively for customers using Workforce Optimization powered by Verint Systems®.

These addresses are required in addition to the [Five9 IP Address Ranges](#).

Location	IP Address
US	34.136.125.118

Location	IP Address
	35.232.209.60
	147.124.190.9
	147.124.190.22
	147.124.190.150
	198.105.200.32/28
	198.105.202.36
Canada	34.95.32.12
	34.95.53.189
	35.203.53.138
	35.203.69.68
	35.203.76.88
EU and UK	34.89.67.65
	34.89.67.66
	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
	35.246.110.38
India	3.33.139.32
	202.92.199.16/28
	202.92.199.80/28

Verint IP Addresses for Global Voice

The additional IP addresses listed below are required with Verint Workforce Optimization for Five9 Global Voice (FGV) customers.

Location	IP Address
Dublin	147.189.19.0/24
Sao Paulo	18.230.120.94
	18.230.253.22
	18.231.18.243

Location	IP Address
	54.232.171.76
	54.233.119.97
	56.125.142.14
	56.125.152.255
	177.71.200.212
Sydney	202.92.193.0/24
Tokyo	202.92.192.0/24

Five9 IP Addresses for VoiceStream

If you implement VoiceStream, ensure that you configure your network and firewall to enable secure SIP and gRPC connections. These addresses are in addition to the [Five9 IP Address Ranges](#).

For more information, see [gRPC Streaming](#), [CTI Call Event Delivery and Authentication](#), and [Receiving Encrypted SIP Audio Streams](#).

Location	IP Address
US/Canada	147.124.160.0/19
EU/UK	147.189.224.0/20
Australia/India/Japan	202.92.198.0/23
Brazil	34.39.142.160/31

Important

You must have a valid publicly-signed certificate, especially when setting a directive to point to an IP address.

VoiceStream CTI Events and Webhooks

There are no IP ranges to add to the allow list for any webhook traffic, and webhooks could originate from anywhere.

Five9 IP Addresses for Workflow Automation and Voice AI Agent

The IP addresses below support the use of Workflow Automation (WFA) and Agent Tools within Voice AI Agent. These addresses are in addition to the [Five9 IP Address](#)

Ranges.

Location	IP Address
US	3.135.6.3/32
	3.150.246.87/32
	3.151.50.213/32
	34.202.119.13/32
	52.202.84.78/32
	98.86.246.238/32
EU	54.216.118.172/32
	63.32.189.56/32
	99.81.238.140/32

Five9 Addresses for Five9 University

Use of Five9 University and Training content is powered by Docebo Learning Management System (LMS) which is supported by AWS Cloudfront (<https://aws.amazon.com/cloudfront/details/>). The AWS Cloudfront distribution addresses Docebo uses for LIVE environments are available at <https://ip-ranges.amazonaws.com/ip-ranges.json>.

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. These addresses are in addition to the [Five9 IP Address Ranges](#).

Five9 Domain	Data Center	URL
five9.com	U.S. data centers	• https://login.five9.com
		• https://api.five9.com
		• https://app.five9.com
		• https://app-scl.five9.com
		• https://app-atl.five9.com
		• https://app.scl.five9.com
		• https://app.atl.five9.com

Five9 Domain	Data Center	URL
		• https://us1.five9.com • https://us8.five9.com • https://us6.five9.com • https://us9.five9.com • https://webstatic.five9.com • https://ws1.five9.com • https://ws8.five9.com • https://ws6.five9.com • https://ws9.five9.com • https://api.prod.us.five9.net • https://cdn.prod.us.five9.net • https://login.auth.five9.com • https://auth.five9.com • https://ssol.auth.five9.com • https://migrate.auth.five9.com • https://admin.us.five9.net • https://webstorage03.five9.com¹ • https://webstorage06.five9.com • https://webstorage08.five9.com • https://webstorage09.five9.com • Shared domains: ◦ https://community.five9.com ◦ https://documentation.five9.com ◦ https://www.five9university.com ◦ https://webswing.prod.us.five9.net
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://app-mtl2.ca.five9.com • https://api.prod.ca.five9.net • https://cdn.prod.ca.five9.net

Five9 Domain	Data Center	URL
		• https://migrate.auth.ca.five9.com • https://admin.ca.five9.net • https://webstatic.ca.five9.com • https://webstorage.ca.five9.com • Shared domains: ◦ https://community.five9.com ◦ https://documentation.five9.com ◦ https://www.five9university.com ◦ https://webswing.prod.us.five9.net
five9.eu	UK data centers (London, London GCP)	• https://login.five9.eu • https://app.five9.eu • https://app-ldn.five9.eu • https://app.ldn1.five9.eu • https://api.five9.eu • https://api.ldn.five9.com • https://api.ldn1.five9.eu • https://eu1.five9.eu • https://eu3.five9.eu • https://env.ldn1.five9.eu • https://webstatic.five9.eu • https://ws1.five9.eu • https://ws3.five9.eu • https://ws1.ldn1.five9.eu • <a href="https://webstorage01.five9.eu<sup>1</sup">https://webstorage01.five9.eu¹ • https://webstorage02.five9.eu • <a href="https://webstorage03.five9.eu<sup>1</sup">https://webstorage03.five9.eu¹ • https://webstorage04.five9.eu • https://webstorage.ldn1.five9.eu • https://api.prod.uk.five9.net • https://cdn.prod.uk.five9.net • https://login.auth.five9.eu • https://auth.five9.eu • https://sso1.auth.five9.eu • https://migrate.auth.five9.eu

Five9 Domain	Data Center	URL
		• https://admin.uk.five9.net • Shared domains: ◦ https://community.five9.com ◦ https://documentation.five9.com ◦ https://www.five9university.com ◦ https://webswing.prod.us.five9.net
eu.five9.com	EU data centers (Frankfurt/ Netherlands in GCP)	• https://login.eu.five9.com • https://admin.eu.five9.net • https://api.eu.five9.com • https://app.eu.five9.com • https://app.frk1.eu.five9.com • https://app.nld1.eu.five9.com • https://env.frk1.eu.five9.com • https://env.nld1.eu.five9.com • https://ws1.frk1.eu.five9.com • https://ws1.nld1.eu.five9.com • https://webstorage.frk1.eu.five9.com • https://webstorage.nld1.eu.five9.com • https://api.prod.eu.five9.net • https://cdn.prod.eu.five9.net • https://migrate.auth.eu.five9.com • Shared domains: ◦ https://community.five9.com ◦ https://documentation.five9.com ◦ https://www.five9university.com ◦ https://webswing.prod.us.five9.net
in.five9.com	India data center	• https://in.five9.com • https://login.in.five9.com • https://admin.in.five9.net • https://app.in.five9.com • https://api.in.five9.com • https://api.prod.in.five9.net • https://app.bom1.in.five9.com • https://app.del1.in.five9.com

Five9 Domain	Data Center	URL
		• https://env.bom1.in.five9.com • https://env.dell1.in.five9.com • https://webstatic.in.five9.com • https://ws1.in.five9.com • https://ws3.in.five9.com • https://webstorage.bom1.in.five9.com • https://webstorage.dell1.in.five9.com • https://cdn.prod.in.five9.net • https://login.auth.five9.com • https://auth.five9.com • Shared domains: ◦ https://community.five9.com ◦ https://documentation.five9.com ◦ https://www.five9university.com ◦ https://webswing.prod.us.five9.net
Five9 UC Adapters - MS Teams and Zoom	U.S. data centers	• https://api.prod.us.five9.net • https://cdn.prod.us.five9.net
	Canada data centers	• https://api.prod.ca.five9.net • https://cdn.prod.ca.five9.net
	EU data centers	• https://api.prod.eu.five9.net • https://cdn.prod.eu.five9.net
	UK data centers	• https://api.prod.uk.five9.net • https://cdn.prod.uk.five9.net
Five9 UC Adapters - RingCentral, Office@Hand, and Nextiva	U.S. data centers	• https://api.prod.us.five9.net • https://cdn.prod.us.five9.net
Digital Engagement administrator console for Plus applications	Santa Clara	https://us8.five9.com/SoCoCare/AdminConsole/#
	Atlanta	https://us9.five9.com/SoCoCare/AdminConsole/#
	London	https://eul.five9.eu/SoCoCare/AdminConsole/#
	London GCP	https://env.ldn1.five9.eu/SoCoCare/AdminConsole/#
Connectivity Assessment Testing	CAT web site	• https://www.five9.com/cat • https://download.visualware.com

¹ Traffic opened to ports 80, 443, 2276, and 2277.

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.

For TCP/UDP requirements for softphone, see [TCP/UDP Port Requirements for Softphone Customers](#).

Depending on your firewall configuration, use one of these methods:

- Create a firewall rule to permit HTTPS connections to these fully-qualified domain names (FQDNs):

- `secure.counterpath.com`
- `secure-east.softphone.com`
- `secure-west.counterpath.com`

or

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

- `216.93.246.0/24` (primary)
- `69.90.51.0/24` (secondary)
- `40.78.10.175`
- `52.183.45.217`
- `52.250.216.127`
- `198.204.63.15`
- `173.244.45.15`

For licensing, add these IP addresses to your list of allowed entities:

- `216.93.246.170`
- `40.78.10.175`
- `52.183.45.217`
- `52.250.216.127`
- `198.204.63.15`
- `173.244.45.15`

WebRTC Requirements

Web Real-Time Communication (WebRTC) enables agents to use their browsers to communicate with customers. Agents do not need to install the softphone plug-in and

an extension because audio and video communications are inside web pages. Not all agents in your domain need to use WebRTC. Agents can use the softphone as needed.

WebRTC is available in US, EU, Canada, India, and Five9 Global Voice (FGV) domains.

For TCP/UDP requirements for WebRTC, see [TCP/UDP Port Requirements for WebRTC Customers](#).

Requirements	Description
Five9 Plus applications	Supervisor Plus, Agent Desktop Plus, and Plus CRM adapters.
WebRTC	Domain enabled.
VDI	See Virtual Desktop Requirements
Network	For US/EU/UK/CA, see Five9 IP Address Ranges for networking requirements by location. Note: For Five9 FGV customers, add the following addresses to your allow list for your locations: • FGV PoP (Dublin) - WebSocket/Agent Registration: 54.73.166.58, 185.111.43.0/24, 212.187.211.0/24 - Media: 54.195.40.249, 63.34.119.26, 185.111.43.0/24, 212.187.211.0/24 • FGV PoP (Sao Paulo) - WebSocket/Agent Registration: 18.229.177.118, 209.14.129.0/24 - Media: 18.228.254.135, 18.230.128.58, 177.71.247.2, 209.14.129.0/24 • FGV PoP (Sydney) - WebSocket/Agent Registration: 13.211.19.119, 103.169.229.0/24 - Media: 52.64.122.16, 3.105.60.140, 103.169.229.0/24 • FGV PoP (Tokyo) - WebSocket/Agent Registration: 3.115.80.118, 103.169.228.0/24 - Media: 18.180.1.110, 54.248.166.76, 103.169.228.0/24

Performance Dashboard

To access Performance Dashboard, firewalls must allow the **clearviewportal.com** domain and sub-domains. The list below shows specific DNS entries and the CNAME (Alias) records as well as the A (Host) record they point to. For the data integrations to

work, the integration IPs must be added to your allow list for Five9 user access if you use an IP allow list.

US East Data Center

UI Access

- CNAME (Alias) <your_domain>clearviewportal.com
- CNAME (Alias) va-five9-root.clearviewportal.com
- A (Host) uiwebalbfive9-1065485923.us-east-1.elb.amazonaws.com

Integration Server IP Addresses

- 34.192.10.54
- 18.212.41.50

US West Data Center

UI Access

- CNAME (Alias) <your_domain>clearviewportal.com
- CNAME (Alias) Oregon-five9-root.clearviewportal.com
- A (Host) uiweboregonfive9-1563430220.us-west-2.elb.amazonaws.com

Integration Server IP Addresses

- 44.231.5.68

Canadian Data Center

UI Access

- CNAME (Alias) <your_domain>clearviewportal.com
- CNAME (Alias) Montreal.clearviewportal.com
- A (Alias) uiwebalb-1155967432.ca-central-1.elb.amazonaws.com

Integration server IP Addresses

- 35.182.166.66
- 35.183.6.253

EU Data Center

UI Access

- CNAME (Alias) <your_domain>clearviewportal.com
- CNAME (Alias) frank.clearviewportal.com
- A (Alias) uiweb-112004485.eu-central-1.elb.amazonaws.com

Integration server IP Addresses

- 18.193.72.36
- 3.125.250.132

UK Data Center

UI Access

- CNAME (Alias) <your_domain>clearviewportal.com
- CNAME (Alias) london-five9-root.clearviewportal.com
- A (Alias) uiweblondonfive9-700149032.eu-west-2.elb.amazonaws.com

Integration Server IP Addresses

- 35.176.128.134
- 52.56.93.155

ClearView is hosted by AWS 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.

For additional requirements for softphone, see [CounterPath Softphone Requirements](#).

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

Port	TCP/UDP	Outbound	Application
			quality.five9.com to verify that your networks are ready to receive Five9 traffic.
8083	TCP		Required by the Five9 Softphone Service. Ensure that no other processes use this port on agent workstations. If you plan to use an http proxy, create an exception for this port on the internal interface. Otherwise, the softphone connection will fail. For instructions, see Web Browser Proxy Configuration. Port 8083 is only required to be open in a host firewall if VDI is required and the DVC plug-in cannot be used for VDI. See Virtual Desktop Requirements.
8843	TCP	Outbound	HTTPS Downloading Five9 applications and API.
8880	TCP	Outbound	HTTP Downloading Five9 applications.

TCP/UDP Port Requirements for WebRTC Customers

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

For additional requirements for WebRTC, see [WebRTC Requirements](#).

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. All ports open for RTP must also allow STUN.

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:

Note

For information about the Five9 NAT gateway idle timeout for UDP sessions, see [Five9 Network Requirements \(LAN and WAN\)](#).

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.
1024-65535	UDP	Outbound	RTP from Five9 Agent Desktop Plus 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 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.

TCP Port Requirements for Five9 Performance Dashboard

To enable agents to connect to the Five9 Performance Dashboard, Wallboard, or Gamification platform, configure the following port:

Port	TCP/UDP	In or Out	Application
443	TCP	Outbound	HTTPS web communication necessary for Five9 Performance Dashboard.

Network Requirements for Five9 Video Engagement

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

Important

When using the SightCall RTCC driver, ensure that the TCP 443 (HTTPS) port is not blocked on your firewall or proxy.

Network Setup For Restricted Networks

If you maintain a restricted network, ensure that the following URL schemes and ports are open:

URL Scheme and Port	Comment
*.rtccloud.net - TCP 443	Required.
*.rtccloud.net - TCP 5204	Optional - used if TCP 443 is blocked.
*.rtccloud.net	Optional - used if TCP 443 is blocked.
*.rtccloud.net - Allow UDP traffic (dynamic port range).	Required if the guest/attendee connects to the call using WebRTC connection mode in the same network used by the agent. This typically occurs during internal testing.
Important: This is highly recommended for better reliability and performance.	
*.sightcall.com - TCP 443	Required.
*.mapbox.com - TCP 443	Required if you use the Geolocation feature in the use cases. For more information, see https://support.sightcall.com/hc/en-us/articles/360056812011-Use-Cases-Configuration-Guide-Console-Controls .

Note

TLS 1.0 and 1.1 are not supported. You must use TLS 1.2.

SightCall recommends allowlisting the **domain name** and not the IP address to account for possible IP address changes in the future. However, if your network only allows IP allowlisting, see: <https://support.sightcall.com/hc/en-us/articles/360049058352-Current-list-of-IP-Addresses-for-SightCall-platforms>.

Media Upload

If you set a media endpoint to receive incoming data and need to allow specific IPs, allow SightCall's entire cloud IP range: 162.252.233.0/24 to account for possible changes in infrastructure in the future. See <https://support.sightcall.com/hc/en-us/articles/360039371652>.

SSL Interception

If you are using Zscaler Cloud Solution or a similar network security solution, **disable** Deep Packet Inspection (DPI) or SSL Inspection for *.rtccloud.net and *.sightcall.com.

Monitoring Internet Bandwidth Usage

To prevent quality problems during video sessions, you should monitor the global network bandwidth usage and SightCall specific usage. Internet usage should never exceed 90% of the link capacity.

The video quality may be temporarily affected by network congestion.

The network bandwidth must be sufficient to support the targeted number of simultaneous video sessions (300-500 kbps per call, depending on the use case).

Implementing Quality of Service (QoS)

Tag SightCall packets as the highest priority streams (real-time) to ensure that they are forwarded as quickly as possible.

Depending on your network configuration, you may need to reserve network bandwidth for video sessions.

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 (see [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

Traffic	Protocol	Ports
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.

Application Usage Analytics

Five9 applications will occasionally send analytics of application usage through <https://aptrinsic.com>. No customer data, personally identifiable information (PII), or keystroke data is sent. Please do not block this data.

Workforce Engagement Management Requirements

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

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

- [Agent Workstation Requirements](#)
- [Supervisor Workstation Requirements](#)
- [Bandwidth Considerations](#)
- [WEM IP Requirements](#)

Agent Workstation Requirements

The following requirements assume that the Five9 VCC and Workforce Engagement Management (WEM) 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](#)
- [Hardware Requirements](#)
- [Operating Systems](#)
- [Web Browsers](#)
- [Software Requirements](#)
- [Configuration Requirements](#)
- [Firewall Policies](#)
- [URLs](#)

Virtualized Agent Environments

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

Hardware Requirements

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.
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-bit and 64-bit)
Windows 10 Home, Pro, and Enterprise	Latest release
Windows 11 Pro and Enterprise	Latest release

Important: Microsoft ended support for Windows 10 on October 14, 2025, and Five9 is no longer testing on that operating system. To avoid any potential service impacts, Five9 strongly recommends upgrading to Windows 11.

Web Browsers

The following web browsers are supported for all WEM components.

Browser*	Version (32-bit)
Google Chrome	Latest release.
Firefox	Latest release.
Edge	Latest release.

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 Antivirus or Antimalware	Exceptions to local antivirus or malware detection applications may be required depending on site-specific policies.

Component	Requirement
	Add the following executables in any antivirus or antimalware 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	WEM CLOUD	443	TCP	Screen capture client HTTPS heartbeat messaging.
Agent PC ¹	WEM CLOUD	22	TCP	Screen capture FTP file transfer.
Agent PC	WEM CLOUD	443	TCP	Application Access.
Agent PC ²	WEM CLOUD	5018	TCP	Live Agent Desktop Access.
Agent PC ²	WEM CLOUD	5019	TCP	Live Agent Desktop Access.
Agent Workstations	VO CLOUD ENV	4443	TCP	Interaction Analytics UI access.
¹ Required only by QM Screen Capture.				
² Required only by QM Live Desktop.				

URLs

WEM requires access to these URLs.

URL	Description
launchdarkly.com	Access to feature management and continuous delivery. For the public IP list for LaunchDarkly, see https://app.launchdarkly.com/api/v2/public-ip-list .
amazonaws.com	Access to AWS Cloud.

Supervisor Workstation Requirements

The following requirements assume that the Five9 VCC and Workforce Engagement Management (WEM) 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](#)

[Hardware Requirements](#)

[Operating Systems](#)

[Web Browsers](#)

[Software Requirements](#)

[Configuration Requirements](#)

[Firewall Policies](#)

Virtualized Supervisor Environments

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

Hardware Requirements

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.
Architecture	32-bit or 64-bit sup-	

Component	Minimum Requirement	Notes
	ported	
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-bit and 64-bit)
Windows 10 Home, Pro, and Enterprise	Latest release
Windows 11 Pro and Enterprise	Latest release

Important: Microsoft ended support for Windows 10 on October 14, 2025, and Five9 is no longer testing on that operating system. To avoid any potential service impacts, Five9 strongly recommends upgrading to Windows 11.

Web Browsers

The following web browsers are supported for all WEM components.

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

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 Antivirus or Antimalware	Exceptions to local AV or malware detection applications may be required depending on site-specific policies. Add the following executables in any antivirus or antimalware program: • <Installation Directory>\voaccli.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	WEM CLOUD	443	TCP	Application Access.
Supervisor/Adm Workstations	VO CLOUD ENV	4443	TCP	Interaction Analytics UI access.

Bandwidth Considerations

Internet bandwidth is used by Five9 Workforce Engagement Management (WEM) 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 WEM cloud environment to the user workstation.

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

[User Media Playback](#)

[Screen Capture Cache Transmission](#)

[Example Screen Capture Calculation](#)

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

Use the following expression 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

WEM IP Requirements

Some WEM services require the following Five9 IP addresses to be added to a list of allowed entities. For details on services, contact your Five9 representative.

US	Canada	London	Frankfurt	India
147.124.167.16	147.124.162.240	147.189.20.196	147.189.18.4	202.92.197.106
147.124.167.119	147.124.162.126	147.189.20.206	147.189.18.33	202.92.197.226
147.124.167.99	147.124.162.235	147.189.20.59	147.189.18.193	202.92.197.126

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