Workspace Desktop Edition Deployment Guide

Workspace SIP Endpoint in Virtual Desktop Infrastructure

4/7/2025

Workspace SIP Endpoint in Virtual Desktop Infrastructure

[**Added:** 8.5.109.16] [**Modified:** 8.5.140.08]

Contents

Important

A direct network connection between the VDI infrastructure (VM or Citrix Server) and Workspace SIP Endpoint host is required. Network Address Translation and home office behind a router without VPN are not supported.

Tip

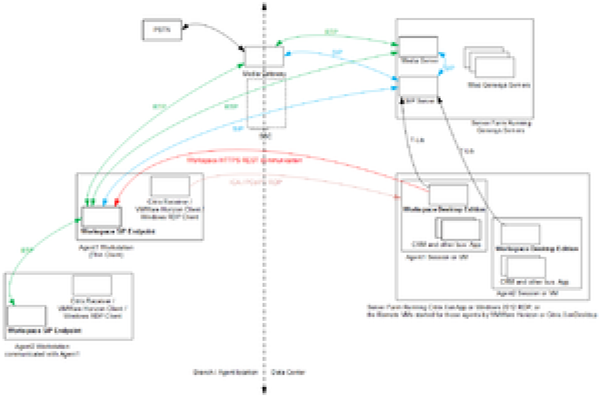
Workspace also supports the Genesys Softphone in place of Workspace SIP Endpoint. To learn about how Genesys Softphone can be deployed in a VDI environment, see Genesys Softphone Deployment Guide.

The standalone version of Workspace SIP Endpoint 8.5.1 enables Workspace and Workspace SIP Endpoint to run in separate user sessions. Workspace manages the UI and interaction control business logic in a virtual desktop infrastructure (VDI, for example: RDP, VMWare, XenApp, XenDesktop) environment and Workspace SIP Endpoint manages voice and video media on the local workstation. This architecture enables you to offload media processing to the agent workstation and reduce the load on your server, leading to better scalability. For information about Virtual Desktop Infrastucture, refer to the Genesys Virtualization Platform Support topics in the *Genesys Supported Operating Environment Reference Guide*.

Workspace SIP Endpoint 8.5.1 can be deployed as a standalone application on agent workstations, either as part of a ClickOnce package or directly installed.

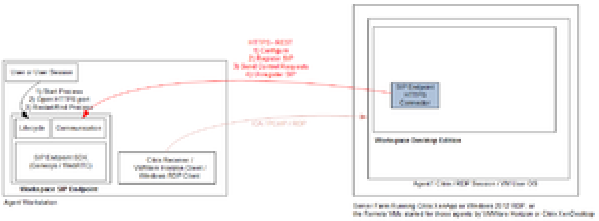
The following figures detail how Workspace and Workspace SIP Endpoint 8.5.1 use HTTPS REST to communicate in a VDI environment. The communication between Workspace and Workspace SIP Endpoint relies on as HTTPS REST connection, independent from the VDI technology.

Network view:



Example of the network connections for Workspace SIP Endpoint Standalone application in a virtualized environment

Component view:



Example of the network connections for Workspace SIP Endpoint Standalone application in a virtualized environment

When Workspace SIP Endpoint is installed as a standalone application on an agent's workstation, its startup and exit are no longer controlled by Workspace. Instead, it is started and stopped as an "auto-start" Windows application and/or manually by the agent.

Provisioning the Workspace SIP Endpoint Standalone mode

By default, Workspace SIP Endpoint is installed as a standalone application with "protocol"="http" and "port"="8000" set.

First install the Workspace SIP Endpoint Standalone application, then provision it in the `InteractionWorkspaceSIPEndpoint.exe.config` file *and* configure the following options in the `interaction-workspace` section of the Workspace Desktop application:

- sipendpoint.standalone.protocol
- sipendpoint.standalone.port
- sipendpoint.standalone.vdi-detection-model
- sipendpoint.standalone.vdi-detection-use-dns [**Added:** 8.5.140.08]
- sipendpoint.standalone.security-level
- sipendpoint.standalone.certificate-search-value
- sipendpoint.standalone.subject-criteria
- sipendpoint.standalone.subject-matching-properties

To adjust these default settings and make Workspace SIP Endpoint 8.5.1 run in standalone mode as a secured application, you must make the following modifications to the SIP Endpoint settings in the appSettings section of the `InteractionWorkspaceSIPEndpoint.exe.config` file:

```
<appSettings>
<!-- This option activates HTTP or HTTPS communication - requires that a port is defined in
port option. -->
<add key="protocol" value="https"/>
<!-- This option gives the level of security if 'protocol' option is set to HTTPS. -->
<!-- 0: check Address IP range, no client certificate required (no check on client
certificate) -->
<!-- 1: check Address IP range, check client certificate -->
<!-- 2: check Address IP range, check client certificate, check client certificate subject -->
<add key="security_level" value="1"/>
<!-- This option gives a string value Workspace uses to select a certificate if 'protocol'
option is set to HTTPS. -->
```

```
<!-- Search is done first by thumbprint, then by issuer, then by subject. -->
<add key="certificate_search_value" value="Communications Server"/>
<!-- This option specifies the port to be used when communicating in HTTP or HTTPS -->
<add key="port" value="8000"/>
<!-- This option is only needed if 'security_level' option is 2 for validation of client
certificate subject. -->
<!-- It gives a list of subject fields to validate in the client certificate. -->
<add key="subject_criteria" value="E,CN,OU,OU,OU,DC,DC,DC,DC"/>
<!-- This option is only needed if 'security_level' option is 2 for validation of client
certificate subject. -->
<!-- It gives a list of current user property values to match with the list of criteria
defined by 'subject_criteria' option. -->
<!-- The certificate subject validation process compare the subject criteria values with
current user property values find in its active directory. -->
<add key="subject_matching_properties"
value="mail,cn,distinguishedName.OU,distinguishedName.OU,distinguishedName.OU,distinguishedName.DC,distinguishe
<!-- This option activates the CORS mechanism for the HTTP REST port with the required policy
-->
<!--<add key="cors" value="*"/>-->
<!-- This option specifies if SIP Endpoint can be activated only by an application on the
same local host -->
<!--<add key="localhost" value="true"/>-->
<!-- These options specify a ranges of IP addresses allowed for connection to SIP Endpoint
http services in CIDR format.-->
<!-- Several range can be applied separted with commas "10.20.35.0/24,10.20.39.0/24"-->
<!--<add key="ipv4_address_range" value=""/>-->
<!--<add key="ipv6_address_range" value=""/>-->
<!-- SIP Endpoint dictionary -->
<add key="title" value="Workspace SIP Endpoint"/>
<add key="exit" value="Exit..."/>
</appSettings>
```

Workspace Standalone SIP Endpoint deployment modes

Workspace Standalone SIP Endpoint can be deployed using one of two modes:

- Standalone Application
- ClickOnce Standalone Package

Standalone mode

In this mode, executing the `setup.exe` file installs Worksapce SIP Endpoint on the target workstation with no pre-requisites other than .NET Framework version 4.5.

It can be executed in silent mode.

You can repackage the out-of-the-box Workspace SIP Endpoint Standalone setup to meet the specifications of "Microsoft System Center Configuration Manager" and allow it to push this software to workstations in a standard way. The auto-start registry keys instructions can be reused for this purpose.

SIP Endpoint auto-start

Workspace SIP Endpoint application is deployed as an auto-start application. This enables the

Workspace SIP Endpoint to be started automatically as a standalone application each time the agent logs in on the workstation, and stops when he or she logs off. To enable this feature, the following registry key is set when Workspace SIP Endpoint is installed:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\
CurrentVersion\Run\InteractionWorkspaceSIPEndpoint
```

The full path to the Workspace SIP Endpoint application is assigned as the value of the this key, for example:

```
C:\Program Files (x86)\InteractionWorkspaceSIPEndpoint\
InteractionWorkspaceSIPEndpoint.exe
```

When the Workspace SIP Endpoint application is running in this mode, the application waits for a Workspace application to connect to the HTTP port and start a SIP session.

Each time that Workspace exits, it informs the connected standalone SIP Endpoint application to finalize its endpoint activity. Once there are no more active calls, Workspace SIP Endpoint closes itself and then restarts so that it is ready to receive a new connection from a new Workspace instance.

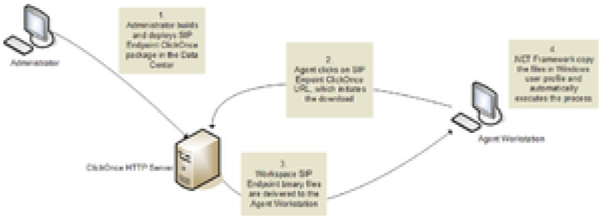
Click-Once mode

Refer to ClickOnce Deployment and Installation.

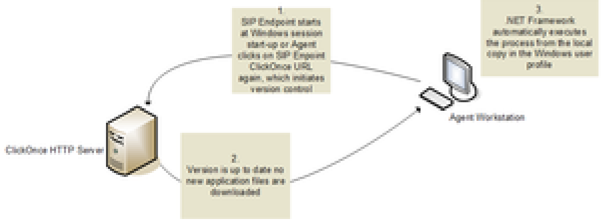
Once Workspace SIP Endpoint is deployed on the HTTP Server, the .NET Framework that is installed as a pre-requisite on Agent Workstation allows a seamless installation as well as execution of the SIP Endpoint process, using only the Microsoft Windows **USER** security model.

The following is a summary of the deployment and upgrade cycle of the Workspace Standalone SIP Endpoint in a ClickOnce deployment:

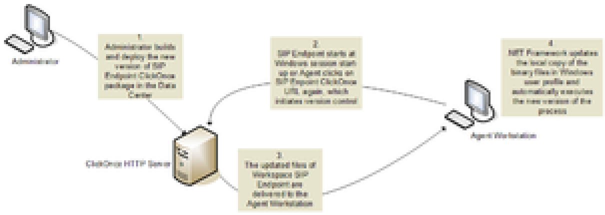
1. First time execution for User X on workstation Y:


Administrator
1. Administrator builds and deploys SIP Endpoint ClickOnce package in the Data Center
2. Agent clicks on SIP Endpoint ClickOnce URL, which initiates the download
4. .NET Framework copy the files in Windows user profile and automatically executes the process
Agent Workstation
ClickOnce HTTP Server
3. Workspace SIP Endpoint binary files are delivered to the Agent Workstation

2. Second time execution for User X on workstation Y, with the server version of the software unchanged:


1. SIP Endpoint starts at Windows session start-up or Agent clicks on SIP Endpoint ClickOnce URL again, which initiates version control
3. .NET Framework automatically executes the process from the local copy in the Windows user profile
Agent Workstation
ClickOnce HTTP Server
2. Version is up to date no new application files are downloaded

3. Third time execution for User X on workstation Y, after the server version of the software has been upgraded:


Administrator
1. Administrator builds and deploy the new version of SIP Endpoint ClickOnce package in the Data Center
2. SIP Endpoint starts at Windows session start up or Agent clicks on SIP Enpoint ClickOnce URL again, which initiates version control
4. NET Framework updates the local copy of the binary files in Windows user profile and automatically executes the new version of the process
Agent Workstation
ClickOnce HTTP Server
3. The updated files of Workspace SIP Endpoint are delivered to the Agent Workstation

Auto-upgrade on ClickOnce in Standalone mode

At Workspace SIP Endpoint application restart, the application checks to determine if a new version is available in the ClickOnce repository, and it is downloaded if necessary. The application is then restarted with the new version.

Auto-start on ClickOnce in Standalone mode

When Workspace SIP Endpoint is installed with ClickOnce as a standalone application, it is then automatically restarted at the beginning of each new Windows session started by the same user on the same workstation.

Workspace Standalone SIP Endpoint security risks

The following table summarizes the various levels of security versus functionality that can be achieved by different option configuration scenarios. Because a dedicated listening port is opened on agent workstations by Workspace Standalone SIP Endpoint, the workstation is vulnerable to certain security risks. This dedicated port is in addition to listening ports that are opened for SIP and RTP/RTCP.

Workspace/SIP Endpoint Security Matrix

Security Level	SIP Endpoint option values	Workspace option values	IT operational effort
Encryption with Validation level 1: no certificate validation (Lab only)	<add key="ipv4_address_range" value=""/> and/or <add key="ipv6_address_range" value=""/> <add key="protocol" value="https"/> <add key="security_level" value="0"/> <add key="certificate_search_value" value="certificate thumbprint"/>	sipendpoint.standalone.security-level=0	**Low**: Make any certificate (valid or not) availalble on the Personal Store of the workstations that run Workspace SIP Endpoint
Encryption with Validation level 2: Simple certificate validation	<add key="ipv4_address_range" value=""/> and/or <add key="ipv6_address_range"	sipendpoint.standalone.security-level=1	**Low**: Make any valid certificate available on the Personal Store of the workstations that

Security Level	SIP Endpoint option values	Workspace option values	IT operational effort
	value=""/> <add key="protocol" value="https"/> <add key="security_level" value="0"/> <add key="certificate_search_value" value="certificate thumbprint"/>		run Workspace SIP Endpoint

Encryption with Validation level 3:
Mutual certificate validation
	<add key="ipv4_address_range" value=""/> and/or <add key="ipv6_address_range" value=""/>
	<add key="protocol" value="https"/>
	<add key="security_level" value="1"/>
	<add key="certificate_search_value" value="certificate thumbprint"/>
		sipendpoint.standalone.security-level=2
		sipendpoint.standalone.certificate-search-value=certificate thumbprint
			Medium:
			Make any valid certificate available on the Personal Store of the workstations that run Workspace SIP Endpoint and on the Personal Store of the virtual system that runs Workspace Desktop Edition

Mutual HTTPS with Personal Identity check	<add key="ipv4_address_range" value=""/> and/or <add key="ipv6_address_range" value=""/> <add key="protocol" value="https"/> <add key="security_level" value="2"/> <add key="certificate_search_value" value="certificate issuer or subject common part"/> <add key="subject_criteria" value="certificate subject attribute for validation, typically 'E'"/> <add key="subject_matching_properties" value="Windows account attribute for validation, typically 'mail'"/>	sipendpoint.standalone.security-level=3 sipendpoint.standalone.certificate-search-value=certificate issuer or subject common part sipendpoint.standalone.subject-criteria=certificate subject attribute for validation, typically 'E' sipendpoint.standalone.subject-matching-properties=Windows account attribute for validation, typically 'mail'	**High**: Make valid personal certificates available on the Personal store of the workstations that run Workspace SIP Endpoint and on the Personal Store of the virtual system that runs Workspace Desktop Edition. The same domain account should be used in both windows sessions. The attributes of the certificate provided by the remote party are compared to the attributes of the local domain user.