Requirements

System Requirements

Important Each of the components listed in the following table must meet the requirements. Use of unsupported components can result in a nonfunctional deployment.

Only the components, platform image versions, and requirements listed in the table are supported.

Component	Requirements
SUSE Linux thin clients—Hardware	**Service Pack 2 (SP2) Platform supported hardware:** Dell Wyse Z50D or D50D **Service Pack 3 (SP3) Platform supported hardware:** Dell Wyse D50Q, Z50Q, or Z50QQ **Note** For information about video resolution and performance, see Video Resolution, on page 3.
SUSE Linux Enterprise Thin Client Platform SP2 Image	11.2.092
SUSE Linux Enterprise Thin Client Platform SP3 Image	11.3.092

Component	Requirements
Hosted virtual desktop OS (server-side)	• Microsoft Windows 7 32 bit • Microsoft Windows 7 64 bit • Microsoft Windows 8 32 bit • Microsoft Windows 8 64 bit • Microsoft Windows 8.1 32 bit • Microsoft Windows 8.1 64 bit • Microsoft Windows 10 32 bit • Microsoft Windows 10 64 bit
Connection broker for the hosted virtual desktop [1]	• Citrix XenDesktop 7.1, 7.5, or 7.6 • Citrix XenApp 6.5, 7.5 or 7.6—Published desktops only • VMware Horizon View 5.3—Published desktops only • VMware Horizon 6.0 (with View)—Published desktops only • VMware Horizon 6 version 6.1.0—Published desktops only
Citrix Receiver or VMware Horizon Client [2] (Installed on the thin client)	The SUSE Linux Enterprise Thin Client Platform SP2 and SP3 images include the required receiver or client.
Cisco Unified Communications client on the hosted virtual desktop • Cisco Jabber for Windows	Cisco Jabber for SUSE Linux 11.5 or 11.6 running on the hosted virtual desktop (HVD). Cisco VXME is compatible with all future 11.5(X) or 11.6(X) Cisco Jabber for Windows versions. For complete information about virtual environment compatibility, see the *Virtual Environments* section in the *Installation and Configuration Guide for Cisco Jabber for SUSE Linux* for your release.

Component	Requirements
Windows Server (Required for Citrix XenApp only)	**Citrix XenApp 6.5** • Microsoft Windows Server 2008 R2 • Windows Server 2008 R2 SP1 (Standard, Enterprise, Datacenter, and Foundation) **Citrix XenApp 7.5 or 7.6** • Microsoft Windows Server 2008 R2 (Standard and Datacenter Editions) • Windows Server 2008 R2 SP1 (Standard, Enterprise, and Datacenter Editions) • Microsoft Windows Server 2012 (Standard and Datacenter Editions)
Cisco Unified Communications Manager	Cisco Unified Communications Manager version 9.x or later
Cisco AnyConnect (Optional)	3.1.08009-71 (available for SP2 and SP3)
Accessories	For a complete listing of supported audio and video accessories, see *Unified Communications Endpoint and Client Accessories*, at http://www.cisco.com/c/en/us/products/unified-communications/uc_endpoints_accessories.html. **Important** Ensure that all Jabra devices are running the latest firmware. You can use Jabra Direct to update the firmware. For more information visit: http://www.jabra.com.

[1] A connection broker is software that creates connections to hosted virtual desktops. A connection broker performs a number of tasks that include

- Validating the username and providing a connection for the user.
- Allowing the user to connect to a specific virtual desktop.

[2] The Citrix Receiver or VMware Horizon Client provides a user interface for the corresponding connection broker.

Video Resolution

Video resolution and performance depend on various factors including the thin client and camera used. The following table lists the maximum expected resolutions for each thin client.

Thin Client Model	Standard Resolution	Resolution With Encoding Camera (Logitech C920-C)
Dell Wyse D50D	up to 240p	up to 480p
Dell Wyse D50Q	up to 480p	up to 720p
Dell Wyse Z50D	up to 360p	up to 720p
Dell Wyse Z50Q	up to 720p	up to 720p
Dell Wyse Z50QQ	up to 480p	up to 720p

Considerations for Thin Clients

SUSE Linux thin clients must meet all system requirements including a compatible base image version. For more information, see *Release Notes for Cisco Virtualization Experience Media Edition for SUSE Linux* for your release.

Wyse Device Manager 5.0 is the recommended deployment tool to deploy VXME to Dell Wyse thin clients.

Important Cisco does not support any management administrative method to deploy VXME to Dell Wyse thin clients. Support for adding and enabling add-ons is provided by Dell Wyse, using Wyse Device Manager or other methods supported by Dell Wyse.

Port Requirements

The following table lists the ports or port ranges used by Cisco Virtualization Experience Media Edition for SUSE Linux.

Table 1: Port Usage

Port	Description
69 and Ephemeral	UDP Outbound traffic for TFTP **Note** An ephemeral port is a short-lived transport protocol port for IP communications. IP software can allocate ephemeral ports automatically from a predefined range. The following protocols can use an ephemeral port assignment for the client end of a communication, to a well-known port on a server. • Stream Control Transmission Protocol (SCTP) • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) A well-known port is a port reserved by the Internet Corporation for Assigned Names and Numbers (ICANN) for assignment for specific applications.
5060	TCP (default) or UDP Outbound traffic for Session Initiation Protocol (SIP) call signaling
5061	TCP Outbound traffic for Secure SIP call signaling
6970	TCP Outbound traffic for HTTP
16384–32767	UDP Inbound and outbound traffic for RTP (audio and video streams) You can configure the Cisco Unified Communications Manager to reduce this port range. Change the **Start/Stop Media Port** setting in the SIP Profile, which is associated with the CSF device.

Important Cisco Virtualization Experience Media Edition uses the computer-telephony integration (CTI) protocol. Cisco Jabber for Windows on a hosted virtual desktop uses outbound TCP port 2748 to connect to the CTI gateway. The CTI gateway is the CTI Manager component of Cisco Unified Communications Manager.

For a complete listing of ports required by Cisco Jabber for Windows, see the planning guide for your release of Cisco Jabber.

Supported Codecs

Table 2: Supported Audio and Video Codecs

Audio Codec	Video Codec
G.722	H.264/AVC

Audio Codec	Video Codec
G.722.1 (24 and 32k) G.722.1 is supported on Cisco Unified Communications Manager 8.6.1 or later.	
G.711 A-law	
G.711 u-law	
G.729a	
Opus Opus is supported on Cisco Unified Communications Manager 11.0 or later.	

AnyConnect Profiles and the Cisco ASA

To enable Cisco AnyConnect connections, set up Cisco AnyConnect profiles on the Cisco Adaptive Security Appliance (ASA). Next, specify the required VPN INI connection parameters on the thin client. After you set up the required profiles and push the INI parameters to the client, users can then establish secure connections.

Before you provide the devices to your remote employees, push the required configuration to the devices on your local network first. You can then provide the preconfigured devices to remote users to operate behind the Cisco AnyConnect VPN.

Profile Setup on Cisco ASA

On the Cisco Adaptive Security Appliance (ASA), AnyConnect profiles provide basic information about connection setup, and users cannot manage or modify them. The profile is an XML file that lets you identify the secure gateway (Cisco ASA) hosts that you want to make accessible. In addition, the profile specifies extra connection attributes and constraints for a user. Usually, a user has a single profile file. This profile contains all the hosts needed by a user, and extra settings as needed.

By creating and assigning different profiles to group policies configured on the Cisco ASA, you can differentiate access to Cisco ASA features. The Cisco ASA automatically pushes the profile assigned to the user upon connection setup.

You can configure a profile using the AnyConnect profile editor, a GUI-based configuration tool launched from the Adaptive Security Device Manager (ASDM). The AnyConnect software package, version 3.0 and later, includes the editor. The editor starts when you load the AnyConnect package on the Cisco ASA as an SSL VPN client image.

For detailed configuration information, see the *Cisco AnyConnect Secure Mobility Client Administrator Guide* for your release.

Cisco AnyConnect Setup Using INI Parameters

To set up Cisco AnyConnect on the device, configure the Custom Connect INI parameter to create Cisco AnyConnect connections. Use the INI parameters to specify the Cisco Adaptive Security Appliance (ASA) address and settings.

Custom Connect Configuration

To create the Cisco AnyConnect connection, configure the Custom Connect parameter in your INI file. The Custom Connect parameter includes a Command option to enable Cisco AnyConnect at startup and to include a Cisco AnyConnect icon on the desktop.

```
CONNECT=Custom \
Description="ASA Connection" \
AutoConnect=Yes \
Reconnect=Yes \
ReconnectSeconds=100 \
Command=/opt/cisco/anyconnect/bin/vpnui
```

Note In the INI file, include the `INIFileSource=cache` parameter. This parameter ensures that devices use the local cached version of the INI file if they cannot access the INI files from Cisco VXC Manager. This parameter is important for devices running the Cisco AnyConnect VPN. These devices require a configuration to reference at bootup before connecting to the network over VPN.

Table 3: Custom Connect Options

Parameter	Description
AutoConnect={no, yes}	**Default is no.** Yes or no option to start a connection automatically at sign-on.
Command=<command or application to be executed from the client>	**Mandatory Option** Specifies a command or application to be executed from the client. For Cisco AnyConnect: Command=/opt/cisco/anyconnect/bin/vpnui
Description=<string description>	**Mandatory Option** Connection description. Provides a connection name for the Desktop icon and the Connection Manager. **Caution** The text must be enclosed in quotation marks if it contains spaces or punctuation characters. These characters are not allowed: & ‘ “ $? ! | ; ( ) [ ] { } \
Reconnect={no, yes}	**Default is no.** Yes or no option to automatically reconnect to an application server after a disconnection.

Parameter	Description
ReconnectSeconds=<value in seconds>	**Default is 30.** Specifies the amount of time in seconds (default is 30) to wait before automatic reconnection to an application server after a disconnection. Requires Reconnect=yes or 1.

Caution Do not insert any additional spaces at the end of lines in the INI file. Extra spaces may cause the device to parse the INI file incorrectly.

INI Parameters for Cisco ASA Settings

To complete the Cisco AnyConnect setup, specify the Cisco ASA address and settings using the following INI parameters. After you configure these settings and the Custom Connect parameter, push the updated INI file to your devices to enable VPN connections.

Table 4: Cisco AnyConnect INI Parameters

Parameter	Description
VPNGroup=<Group name>,... (optional)	Use this parameter if you configure groups on the Cisco ASA. This parameter specifies the name or names (separated by commas) that the Cisco AnyConnect Client can use for the VPN connection.
VPNHeadendAddress= <FQDN or IP address> (required)	Specifies the VPN headend FQDN or IP Address to autoconfigure the Cisco AnyConnect Client. For example, VPN.Cisco.com or 192.168.0.1.

The following shows an example configuration:

```
VPNGroup= profilename
VPNHeadendAddress=192.168.0.1
```