Connectivity options configuration

- Global Connection Settings dialog box, page 1
- Connectivity options access, page 5
- Advanced details about ICA and RDP connections, page 18

Global Connection Settings dialog box

Tip
While it is not recommended to use dialog boxes for configuring zero client connection settings, they are available in case you want to temporarily override central default configurations or you do not have the option to set up central configuration (smaller environments). In general, it is recommended that you use central configuration to enable you to automatically push updates and any desired default configuration to all supported zero clients in your environment.

If you do not use INI files to provide central configuration (global connection settings) to users, you can use the Global Connection Settings dialog box (Home icon > Global Connection Settings) to configure settings that affect all of the connections in your list of connections.

- Cisco VXC desktop: click Global Connection Settings in the List of Connections
- Classic Desktop: click Global Connection Settings in the Connect Manager

Tip
For information on configuring the zero client using INI files (recommended), see INI Files Reference Guide for Cisco Virtual Experience Client 2112/2212.
**Session tab**

The following figure shows the Session tab.

**Figure 1: Session tab**

Use the Session tab to select the check boxes you want for the options that are available to all sessions (the Smart Cards check box specifies the default setting for connecting to a smart card reader at startup).

**Tip**
ICA sessions always have automatic connection to attached smart card readers.

When using the Disks check box for automatic connection to connected USB sticks, use the following guidelines:

- Support is for VFAT File System only; be sure that the USB stick you use is formatted to FAT16 or FAT32.
- More than one disk can be used at the same time, however, the maximum number of USB sticks (including different subareas) is 12.
- It recommended that you use Windows XP, Windows Server 2003, or Windows Server 2008 for the server.
- Be sure to save all data and sign off from the session mapping the USB stick before removing the USB stick.

**Note**
- Granular Control over USB Redirection - By default, audio, video, and printer devices will not use HDX USB for redirection. You can make selections for USB device redirection on the Session tab of the Global Connection Settings dialog box.
- For Web camera mapping, if the server does not support HDX USB redirection and you set this mode in the client, the client will use HDX Realtime Webcam Compression.
ICA tab

The following figure shows the ICA tab.

*Figure 2: ICA tab*

Use the ICA tab to select the check boxes you want for the options that are available to all ICA sessions. Select the audio quality optimized for your connection.

Note the following:

- **Map to**—When a drive is entered, maps a disk under the drive.
- **Map all disks under**—When selected, you can use the drop-down list to select the drive under which you want to map all disks.

RDP tab

The following figure shows the RDP tab.
Use the RDP tab to:

- Enable or disable Network Level Authentication (NLA). The NLA authentication method verifies users before they are allowed to connect with a full Remote Desktop connection.

**Note**

For users to be able to log in to an RDP session when the AD policy is set to change password on first logon, the following configuration is required:

- On the Cisco VXC device, uncheck **Enable NLA**.
- On the RDP server, uncheck **Allow connections only from computer running Remote Desktop with NLA**.

This configuration is also required to display more descriptive errors (other than an authentication failure) when a user enters an incorrect username/password.

- Enable or disable ForceSpan. This dual-monitor feature allows you to span the session horizontally across two monitors (two monitors acting as one large monitor).
- Enable or disable Terminal Service Multimedia Redirection (TSM).
- Enable or disable Record from Local (recording from local microphone).
- Enable or disable RemoteFX.
- Select the USB Redirection Type (TCX USB or RDP USB). TCX USB is the default. To use RDP USB you must use a RemoteFX session (RDP USB is not supported using a standard RDP session).

**Note**

TCX USB is not supported on the Cisco VXC 2112/2212.
Connectivity options access

You can configure the Connectivity options using zero client dialog boxes (depending on user privilege level, some options may not be available for use).

Tip

While it is not recommended to use zero client dialog boxes for configuring Connectivity options, they are available in case you want to temporarily override central default configurations or you do not have the option to set up central configuration (smaller environments). In general, it is recommended that you use central configuration to enable you to automatically push updates and any desired default configuration to all zero clients in your WTOS environment.

To access Connectivity options:

- Cisco VXC desktop—click the System Settings icon on the Cisco VXC toolbar (administrators can also click the Admin Mode button in the Login dialog box).

*Figure 4: System Settings menu*

- Classic Desktop—click UserName (UserName is the name of the user who is logged in and the name is displayed at the bottom-left side of the task bar), and select System Setup.

*Figure 5: Desktop menu*
Network Setup

The Network Setup dialog box (System Settings icon > Network Setup) allows you to configure zero client network settings.

Tip

If required by the operating environment, the network administrator may disable access to this dialog box. Specifically, it cannot be accessed by Low-privileged and Non-privileged users. For more information, see Enabling the disabled Network Setup dialog box, on page 12.

General tab

The following figure shows the General tab.

Figure 6: General tab

Use the following guidelines for the General tab:

• Ethernet Speed—Normally the default (Auto-Detect) should be selected, but another selection can be made if automatic negotiation is not supported by your network equipment. Selections include Auto-Detect, 10 Mb Half-Duplex, 10 Mb Full-Duplex, 100 Mb Half-Duplex, and 100 Mb Full-Duplex.

Tip

The 10 Mb Full-Duplex option can be selected locally at the device; however, this mode may need to be negotiated through Auto-Detect.

• IPV4 - Properties command button:

  ° Dynamically allocated over DHCP/BOOTP—Selecting this option enables your zero client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server (using DHCP options) to provide information. Any value provided by the DHCP server will replace any value entered locally on the Options tab, however, locally entered values will be used if the DHCP server fails to provide replacement values.
• **Statically specified IP Address**—Select this option to manually enter the IP Address, Subnet Mask, and Default Gateway:

  • **IP Address**—Must be a valid network address in the server environment. The network administrator must provide this information.

  • **Subnet Mask**—Enter the value of the subnet mask. A subnet mask is used to gain access to machines on other subnets. The subnet mask is used to differentiate the location of other IP addresses with two choices: same subnet or other subnet. If the location is other subnet, messages sent to that address must be sent through the Default Gateway, whether specified through local configuration or through DHCP. The network administrator must provide this value.

  • **Default Gateway**—Use of gateways is optional. Gateways are used to interconnect multiple networks (routing or delivering IP packets between them). The default gateway is used for accessing the Internet or an intranet with multiple subnets. If no gateway is specified, the thin client can only address other systems on the same subnet. Enter the address of the router that connects the thin client to the Internet. The address must exist on the same subnet as the thin client as defined by the IP address and the subnet mask. If DHCP is used, the address can be supplied through DHCP.

• **IPV6**—Advanced command button: Allows you to select various setting options supported by IPV6.

• **IPV6 - Properties command button:**

  • **Wait DHCP**—Selecting this option enables your zero client to wait for IPV6 DHCP before signing on (if not selected the system will only wait for IPV4 DHCP if enabled).

  • **Dynamically allocated over DHCP/BOOTP**—Selecting this option enables your zero client to automatically receive information from the DHCP server. The network administrator must configure the DHCP server (using DHCP options) to provide information. Any value provided by the DHCP server will replace any value entered locally on the Options tab, however, locally entered values will be used if the DHCP server fails to provide replacement values.

• **Statically specified IP Address**—Select this option to manual enter the IP Address, Subnet Mask, and Default Gateway:

  • **IP Address**—Must be a valid network address in the server environment. The network administrator must provide this information.

  • **Subnet Mask**—Enter the value of the subnet mask. A subnet mask is used to gain access to machines on other subnets. The subnet mask is used to differentiate the location of other IP addresses with two choices: same subnet or other subnet. If the location is other subnet, messages sent to that address must be sent through the Default Gateway, whether specified through local configuration or through DHCP. Ask the network administrator for this value.

  • **Default Gateway**—Use of gateways is optional. Gateways are used to interconnect multiple networks (routing or delivering IP packets between them). The default gateway is used for accessing the Internet or an intranet with multiple subnets. If no gateway is specified, your zero client can only address other systems on the same subnet. Enter the address of the router that connects your zero client to the Internet. The address must exist on the same subnet as your zero client as defined by the IP address and the subnet mask. If DHCP is used, the address can be supplied through DHCP.
• DNS Servers—Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than DNS will be used to make the connection. Enter the network address of an available DNS Server. The value for this box may be supplied by a DHCP server. If the DHCP server supplies this value, it will replace any locally configured value. If the DHCP server does not supply this value, the locally configured value will be used.

Tip
You may enter two DNS Server addresses, separated by a semicolon, comma, or space. The first address is for the primary DNS server and the second is for a backup DNS server.

• Tcp Timeout—Enter the number that is multiplied by 30 seconds for the timeout value of a TCP connection. The value must be 1 or 2 which means the connection timeout value is from 1x30= 30 seconds to 2x30= 60 seconds.

• Show WAN configuration on System Settings—Allows you to show the WAN configuration on the System Settings submenu.

Name Servers tab

The following figure shows the Name Servers tab.

Figure 7: Name Servers tab

Use the following guidelines for the Name Servers tab:

• DNS Domain and DNS Servers—Use of DNS is optional. DNS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than DNS will be used to make the connection. Enter the DNS Domain and the network address of an available DNS Server. The function of the DNS Domain entry is to provide a default suffix to be used in name resolution. The values for these two boxes may be supplied by a DHCP server. If the DHCP server supplies these values, they will replace any locally configured values. If the DHCP server does not supply these values, the locally configured values will be used.
You may enter two DNS Server addresses, separated by a semicolon, comma, or space. The first address is for the primary DNS server and the second is for a backup DNS server.

**Tip**

- WINS Servers—Use of WINS is optional. Enter the network address of an available WINS name server. WINS allows you to specify remote systems by their host names rather than IP addresses. If a specific IP address (instead of a name) is entered for a connection, it rather than WINS will be used to make the connection. These entries can be supplied through DHCP if DHCP is used. DNS and WINS provide essentially the same function, name resolution. If both DNS and WINS are available, the zero client will attempt to resolve the name using DNS first and then WINS.

You may enter two WINS Server addresses (primary and secondary), separated by a semicolon, comma, or space.

**Options tab**

The following figure shows the Options tab.

*Figure 8: Options tab*

Use the following guidelines for the Options tab:

- **DHCP Option IDs**—Enter the supported DHCP options (each value can only be used once and must be between 128 and 254).
- **Interpret DHCP Vendor-Specific Info** - Automatically interprets Vendor information.
- **DHCP Vendor ID**—Shows the DHCP Vendor ID when the Dynamically allocated over DHCP/BOOTP option is selected.
- **DHCP UserClass ID**—Shows the DHCP UserClass ID when the Dynamically allocated over DHCP/BOOTP option is selected.
Related Topics

Direct thin client to server using DHCP

Security tab

The following figure shows the Security tab.

\textit{Figure 9: Security tab}

Use the following guidelines for the Security tab:

- Enable IEEE 802.1x authentication—Select this check box to enable this authentication and activate the EAP Type list of options.

- EAP Type—If you have enabled the Enable IEEE 802.1x authentication check box, select the EAP Type option you want (TLS, LEAP, or PEAP).
  
  - TLS—If you select the TLS option, click \textit{Properties} to open and configure the Authentication Properties dialog box (you can use Browse to find and select the Client Certificate file and Private Key file you want). Validate Server Certificate is mandatory (be sure the check box is checked). Note that the CA certificate must be installed on the zero client. Also note that the server certificate text field supports a maximum of approximately 127 characters, and supports multiple server names.

  The following kinds of server names are supported (all examples are based on Cert Common name is "company.cisco.com").

\textbf{Note}

Using only the FQDN (for example, company.cisco.com) will not work, you must use one of the options (note that *.cisco.com is the most common option as multiple authentication servers may exist):

- servername.cisco.com
- *.cisco.com
- *cisco.com
- *.com
LEAP—If you select the LEAP option, click Properties to open and configure the Authentication Properties dialog box (be sure to use the correct username and password for authentication). Note that the maximum length for the username or the password is 64 characters.

PEAP—If you select the PEAP option, click Properties to open and configure the Authentication Properties dialog box (be sure to select either EAP_GTC or EAP_MSCHAPv2, and then use the correct Username, Password, and Domain, if necessary, for authentication). Validate Server Certificate is optional. Note that the server certificate text field supports a maximum of approximately 127 characters and supports multiple server names.

The following kinds of server names are supported (all examples are based on Cert Common name is "company.cisco.com").

Note Using only the FQDN (for example, company.cisco.com) will not work, you must use one of the options (note that *.cisco.com is the most common option as multiple authentication servers may exist):

- servername.cisco.com
- *.cisco.com
- *.cisco.com
- *.com
- *

To configure EAP-GTC, enter the username only, and the password or PIN will be asked when authenticating. To configure EAP-MSCHAPv2, enter the username, password, and domain (domain\username in the username box is supported, but you must leave the domain box blank). Note that the CA certificate must be installed on the zero client (the server certificate is forced to be validated). Also note that when EAP Type EAP-MSCCHAPV2 is selected on the Authentication Properties dialog box (for PEAP IEEE802.1x authentication), an option to hide the domain is available for selection (the Username and Password text boxes are available for use, but the Domain text box displays gray).

Certificate Management—Opens the Certificates Browser where you can select the Import From option you want to import a certificate (either USB Storage or File Server).

- USB Storage—If you select the USB Storage option, click Import to open and use the Import dialog box to find and select the certificate you want to use. The maximum importing path is limited to 128 characters and the maximum certificate name is limited to 64 characters.

- File Server—If you select the File Server option, click Import to open and use the Import dialog box to enter the detailed path to the certificate you want to use in the File Servers box (if necessary, be sure to use the correct Username and Password). Note that you must enter the absolute path of the certificate. For example: 10.151.121.100/wnos/cacerts/mycertificate.cer. The maximum importing path is limited to 128 characters and the maximum certificate name is limited to 64 characters.
Alternative to Cert Common Name in server certificate field

If you want to use a name other than the Cert Common Name in the server certificate field (for TLS or PEAP authentication) you must customize the certificate with a Subject Alternative Name, specifying for example an IP address or other FQDN. The following figure shows an example of a customized certificate.

**Figure 10: Customize certificate example**

After you customize the certificate, you can enter any value that is specified in the Subject Name or Subject Alternative Name of the certificate into the server certificate field. The client trusts the server certificate if the value specified in the server certificate field matches the Subject Name (CN) or the Subject Alternative Name (SAN) field.

Enabling the disabled Network Setup dialog box

Although there are privileges and user modes associated with user access to zero client resources, access to network setup (using the Network Setup dialog box) depends upon privilege level. A Standalone user either is by default a user with High privilege or has a zero client that is locked down. A Guest user has an implicit privilege of None and all access is governed by that privilege. A PNAgent/PNLite-only user has whatever privilege was set in the wnos.ini file at zero client boot, whatever privilege was locked down at the last access of a wnos.ini file, or High privilege (by default).

If the Privilege parameter is set to Low or None in the INI files, the zero client Network Setup dialog box will be disabled (the user cannot access it). In such a case, there may be occasion to access the Network Setup
dialog box without wanting to change the INI files. For example, an occasion when you need to change to another FTP or Virtual Desktop file server or add to the PNAgent/PNLite servers list. To access the Network Setup dialog box in such a case, disconnect the network cable and reboot the zero client to Standalone user mode. The Network Setup dialog box displays after the zero client initializes and you can then make the required entries (be sure to reconnect the network cable and reboot when finished).

Remote connection setup

Use the Remote Connections dialog box (**System Settings icon > Remote Connections**) to configure zero client remote connections (including ICA, RDP, Citrix XenDesktop, and other broker server connections), visual options, and general connection settings.

**Tip**
In the Classic Desktop option, the Remote Connections dialog box allows you to create default ICA and RDP connections for use. If you want to create several ICA and RDP connections (more than the default connections), use the Connect Manager (see **Connect Manager**).

Broker Setup tab

The following figure shows the Broker Setup tab.

*Figure 11: Broker Setup tab*

Use the following guidelines for the Broker Setup tab:

**Tip**
Locations can be supplied through a wnos.ini file if it is used. If DHCP is used, locations can be supplied through DHCP. After creating an entry, be sure to reboot the zero client to have the changes take effect.
• Citrix Xen Connection (Recommended option)—Select **Citrix Xen**, enter the IP address for the server in the Broker Server box, select your options, and then click **OK**.

Use the following guidelines for the Citrix Xen Broker Server:

* Enter the IP Address or host name for the server in the Broker Server box.

* Use the **Enable automatic reconnection at logon** and **Enable automatic reconnection from button menu** check boxes and options to further configure the connection for automatic reconnection.

* (HTTPS only) Use the Account Self-Service Server box to enter the Account Self-Service IP address such as https://IPAddress. Locations can be supplied through a wnos.ini file if it is used. If DHCP is used, locations can be supplied through DHCP. After making an entry, be sure to reboot the zero client to have the changes take effect. This feature allows users to change or reset their own password and to unlock their account from the Login dialog box (see **Login dialog box features**).

**Note**

The account self-service feature requires the usage of Citrix Password manager.

* Use the XenApp button to use your default settings for the XenApp default settings (IMPORTANT: Note that the system will restart to apply the new settings).

* Use the XenDesktop button to use your default settings for the XenDesktop default settings (IMPORTANT: Note that the system will restart to apply the new settings).

* After entering the information above, the user must reset the Cisco VXC client for the client to find the broker server for login. When the Cisco VXC client is configured in this way, the system administrator generally does not need to configure any other settings. All other settings have the required defaults.

• ICA Connection—Select **None**, select **ICA**, click **Configure Connection**, and then follow the wizard (see **ICA connection setup**, on page 19).

• RDP Connection—Select **None**, select **RDP**, click **Configure Connection**, and then follow the wizard (see **RDP connection setup**, on page 23).

• Microsoft Connection—Select **Microsoft**, enter the IP Address for the server in the Broker Server box, and then click **OK**.

• Dell vWorkspace Connection

**Note**

The Cisco VXC 2112/2212 does not support Dell vWorkspace connections.

• VMware View Connection—Select **VMware View**, enter the IP Address for the server in the Broker Server box, select the Security Mode you want (to verify the identity of the servers to which it connects), and then click **OK**.

• Direct Connection—Select **Other**, enter the IP Address for the broker server in the Broker Server box, and then click **OK**.
The broker supports both HTTP and HTTPS, and depends on the broker server support. If HTTP or HTTPS is not specified on the broker server, then HTTP is used by default. If HTTPS is specified, the client side must install a corresponding root certificate locally.

**Related Topics**

HTTPS/SSL server setup

**Visual Experience Tab**

The following figure shows the Visual Experience tab.

*Figure 12: Visual Experience tab*

Use the following guidelines for the Visual Experience tab:

- **Classic Desktop**—Displays the full task bar, desktop, and Connect Manager familiar to WTOS users. This option is recommended for terminal server environment.

- **Zero Launchpad**—Displays the launchpad-style Cisco VXC desktop GUI designed for VDI use. Functionality is accessed through an always available interface. This option is recommended for VDI and any full-screen-only connections.

- Toolbar, hot key, and connection icon options are also available for configuration.

**General Options tab**

The following figure shows the General Options tab.
Use the General Options tab options to select the action after you exit all open desktops (by default, the zero client automatically returns to the Login dialog box and is ready for another user), to set the default sign-on credentials (Username, Password, and Domain), to set the One Sign Server Virtual Desktop Access, and to clear locally saved connections (use the Clear locally saved connections button to clear connections you no longer need).

If you enter all three Default Sign-on credentials (Username, Password, and Domain), you will be automatically logged on to your desktop upon system start.

The OneSign Server field is for use with the Imprivata OneSign Server, which Cisco does not support. For user authentication on the Cisco VXC 2111/2211, Cisco supports only Gemalto .NET Smart cards. For detailed information, see [http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/VXI_GemaltoNET.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/VXI_GemaltoNET.pdf)

The Wtos firmware supports additional smart cards, but Cisco does not provide support for these smart card solutions. For additional information about smart cards, contact your smart card vendor.
Central configuration setup

The Central Configuration dialog box allows you to configure zero client central connection settings such as file server and optional VXC Manager server settings.

Figure 14: Central Configuration dialog box

Use the following guidelines:

- **File Servers/Path, Username, and Password**—IP address or host name of the file server that provides the system software and update images. The address can be supplied through DHCP if DHCP is used. Use the following guidelines:
  - **File Servers/Path**—Allows 128 characters maximum. The data specifies part of the path to be used when the server is accessed. Multiple file servers/paths may be named, as long as all data fits in the length limitation.
  - **Username**—To log in to the file server. Use 15 characters maximum.
  - **Password**—To log in to the file server. Use 15 characters maximum.
VXC-M tab

Use the following guidelines

VXC-M Servers - List of IP addresses or host names if Cisco VXC Manager is used. Locations can also be supplied through user profiles if user INI profiles are used.

- Discovery Settings area (For more information on setting up the discovery options, see the Installation Guide for Cisco Virtualization Experience Client Manager):
  - DNS Name Record - (Dynamic Discovery) Allows devices to use the DNS Hostname lookup method to discover a Cisco VXC Manager Server.
  - DNS SRV Record - (Dynamic Discovery) Allows devices to use the DNS SRV record lookup method to discover a Cisco VXC Manager Server.
  - DHCP Inform - (Dynamic Discovery) Allows devices to use DHCP option tags to discover a Cisco VXC Manager Server.
  - Manual Discovery in Management Console - (Manual Discovery from Cisco VXC Manager) If no Dynamic Discovery method is used, you can use the Find Devices dialog box to discover devices from Cisco VXC Manager (Cisco VXC Manager Agents will respond to the server discovery by storing the discovered Web Server IP address and port and begin regular check-ins).
  - Enable Automatic Discovery After Missed Check-ins - Select the number of missed check-ins after which you want the auto discovery options enabled.

Note
The Cisco VXC 2112/2212 does not support configuration of the Cloud Client Manager Service using the CCM tab.

Advanced details about ICA and RDP connections

Use the following information when configuring ICA and RDP connections (this information assumes that the zero client does not have a locked down privilege level):
• High-privileged user—The additional functionality provided by the Connection Settings dialog box allows testing of connection definitions before they are entered (by a network administrator) into the user profile files.

• Low-privileged user—The settings for the selected connection can be viewed but cannot be edited, and new connections cannot be defined. Connection definitions are controlled by a network administrator and are accessed by the zero client from the user profiles located on a remote server.

• Standalone user—The Connect Manager is available to Standalone users because connection definitions cannot be accessed from remote user profiles. If user profiles are available on an FTP server but are not accessed because DHCP is not available or is not configured to provide the file server IP address, the file server IP location can be entered manually using the Network Setup dialog box.

ICA connection setup

The following sections provide information about configuring ICA connections.

Connection tab

The following figure shows the Connection tab.

*Figure 15: Connection tab*

If you select the **Server** option, the Host Names box is displayed.
If you select the **Published Application** option, the Application Name box replaces the Host Names box.

*Figure 16: Connection tab: Published Application*

Use the following guidelines on the Connection tab:

- **Server or Published Application**—Select the type of connection to which the settings apply.

- **Connection Description**—Enter the descriptive name that is to appear in the connection list (38 characters maximum).

- **Browser Servers IP**—Enter a delimited (comma or semicolon) list of IP addresses or DNS-registered names of ICA servers that contains the master browsers list, or that could refer to another server that contains the list. The master browsers list is generated automatically by a browsing program on one of the ICA servers (selected by negotiation between servers). It is used to provide the information displayed in the Server Name or IP box. No entry is needed if the list is on an ICA server in the same network segment as the zero client. No entry is necessary if the connection is to a server, or if the server name or IP contains the IP address of the server.

- **HostName or Application Name** (title depends on the Server or Published Application option selected)—You can enter a delimited (semicolon or comma separated) list of server host names or IP addresses, or you can select from the list of ICA servers or published applications (depending on Server or Published Application option selected) obtained from the ICA master browser (you can also use Browse next to the box to make the selection you want). If you enter a delimited list of servers, the zero client attempts to connect to the next server on the list if the previous server attempt failed. If you use the list and the selected connection fails, the zero client attempts to connect to the next one on the list.

**Tip**

The Host Name may be resolved using one of three mechanisms: ICA master browser, DNS, or WINS. Master browser is the only mechanism that can resolve a published application (unless manual entry is made in DNS for the application). DNS uses the default domain name in the network control panel to attempt to construct an FQDN but will also try to resolve the name without using the default.
• Encryption Level—Allows you to select the security level of communications between the zero client and the ICA server. Basic (the default option) is the lowest level of security. Basic allows faster communication between the device and the ICA server because it requires less processing than do the higher levels of encryption.

⚠️ Caution

The encryption selection applies to the security of communications between the zero client and the ICA server only. It is independent of the security settings of individual applications on the ICA server. For example, most Web financial transactions require the zero client to use 128-bit encryption. However, transaction information could be exposed to a lower level of security if the zero client encryption is not also set to 128 bits.

• Use HTTP for browsing—When selected, the zero client, by default, uses http when browsing.

• Alternate address via firewall—When selected, the zero client will use an alternate IP address returned from the ICA master browser to get through firewalls. Used for the Windows log-on when the connection is activated.

• Display Resolution—Select the display resolution for this connection (if you select the Published Application option, the Connection Display will allow you to select the Seamless Display Resolution option).

• Colors—Select the color depth of the ICA session. If High Colors (16bits) or True Colors is selected and the ICA server does not support this color depth, the zero client renegotiates the color depth to the lower value (for example, 256 Colors [8 bits]).

• Window mode and Full screen mode—Select the initial view of the application in a windowed screen or full screen. You can toggle between viewing modes by using Ctrl-Alt-Up Arrow.

• Auto-connect on start-up—When selected, automatically connects the session on start-up.

• Re-connect after disconnect—When selected, causes the zero client to automatically reconnect to a session after a non-operator-initiated disconnect. If selected, the wait interval is that set in the Delay before re-connecting box (enter the number of seconds 1 to 3600) or the user profile for yes (20 seconds) or seconds. The default is 20 seconds if there is no INI file description of this connection, or is a Standalone user, or simply omitted.

### Logon tab

The following figure shows the Logon tab.
Use the following guidelines on the Logon tab:

- **Logging on area**—Enter Login Username, Password, Domain name, and Logon Mode (if the Login Username, Password, and Domain name boxes are not populated, you can enter the information manually in the ICA server login screen when the connection is made):
  - Login Username—31 characters maximum.
  - Password—19 characters maximum.
  - Domain Name—31 characters maximum.
  - Logon Mode—Select User-specified credentials, Smart Card, or Local User.

- **Start Command area**—(Server Connection Option Only—This area is disabled (grayed) for a Published Application option.)
  - Application (127 characters maximum) and Working Directory (63 characters maximum)—Enter an initialization string and arguments, including an associated working directory, that you want to start automatically on the server when the connection is made.

**Options tab**

The following figure shows the Options tab.
Use the following guidelines on the Options tab:

- **Auto-connect to local devices**—Select any options (Printers, Serials, USB, Smart Cards, Sound, and Disks) to have the zero client automatically connect to the devices (an ICA session will not automatically connect to a device through a serial port).
- **Turn compression off**—When selected, turns compression off (intended for high-speed connections).
- **Optimize for low speed link**—When selected, allows optimization for low-speed connections, such as reducing audio quality or decreasing protocol-specific cache size. Intended for a connection spanning a WAN link or using dialup.
- **Enable session reliability**—When enabled, session reliability allows a user to momentarily lose connection to the server without having to re-authenticate upon regaining a connection. Instead of a user’s connection timing out after X seconds, the session is kept alive on the server and is made available to the client upon regaining connectivity.
- **Allow font smoothing**—When selected, enables font smoothing (smooth type).

**RDP connection setup**

In a Virtual Desktop environment, an RDP connection will be assigned by the Virtual Desktop Broker; you do not need to create an RDP connection manually. The Virtual Desktop Broker virtual machine can be reset from the zero client by opening the Connection Settings dialog box of the virtual machine, and then clicking the reset button (appears in the top-right of the dialog box).

**Connection tab**

The following figure shows the Connection tab.
Use the following guidelines on the Connection tab:

• **Connection Description**—Enter the descriptive name that is to appear in the connection list (38 characters maximum).

• **Host Names**—Use the list to select the valid DNS server name or the IP address of the server to which the zero client connection is to be made (you can also use Browse next to the box to make the selection you want). For example, a list of WTS servers on the local network from which you can select.

  **Tip** The server name may be resolved using one of two mechanisms: DNS, and WINS. DNS uses the default domain name in the network control panel to attempt to construct an FQDN but will also try to resolve the name without using the default.

• **Console mode**—Select to set the RDP connection with Windows Console mode.

• **Display Resolution**—Select the display resolution for this connection:

  • **Colors**—Select the color depth of the RDP session. If High Colors (16 bits) or True Colors (32 bits) is selected and the RDP server does not support this color depth, the zero client renegotiates the color depth to the lower value, for example, 256 Colors (8 bits). The highest is 32 bits, if hardware supports it.

  **Tip** For some zero clients versions, only the 256 Colors (8 bits) selection is available for RDP connections. Also, for older versions of the server software (for example, RDP 4.0) the server supports only 8 bit color. This is not detectable in advance but results in use of 8-bit color when the connection is established.

• **Full screen on 1 monitor and Span both monitors**—Select the initial view of the application in a full screen or span. You can toggle between viewing modes by using Ctrl-Alt-Up Arrow.

• **Auto-connect on start-up**—When selected, automatically connects the session on start-up.
• Re-connect after disconnect—When selected, causes the zero client to automatically reconnect to a session after a non-operator-initiated disconnect. If selected, the wait interval is that set in the Delay before re-connecting box (enter the number of seconds 1 to 3600) or the user profile for yes (20 seconds) or seconds. The default is 20 seconds if there is no INI file description of this connection, or is a Standalone user, or is simply omitted.

Tip You can reset the options on the Connection tab of the Connection Settings (RDP) dialog box. To do so, click the Reset VM command button. This command button is located in the upper-right of the dialog box. It appears only with a VDM broker connection.

Logon tab

The following figure shows the Logon tab.

Figure 20: Logon tab

Use the following guidelines on the Logon tab:

• Logging on area—Enter login username, password, and domain name. If these boxes are not populated, you can enter the information manually in the RDP server login screen when the connection is made. Use the following guidelines:

  ◦ Login Username—31 characters maximum.
  ◦ Password—19 characters maximum.
  ◦ Domain Name—31 characters maximum.

• Application (127 characters maximum) and Working Directory (63 characters maximum)—Enter an initialization string and arguments, including an associated working directory, that you want to start automatically on the server when the connection is made.
• Use TS Gateway—Enables the use of Terminal Services Gateway (TS Gateway) server when connecting. If required, then enter the IP address or URL of the TS Gateway server in the Server name box. You can also enable Use Same Info (if the server credentials are the same credentials as your Remote Desktop Credentials (Host remote computer credentials) in the Login Username, Password, and Domain name fields) or disable Use Same Info and enter the Server name, User name, Password, and Domain name of the TS Gateway server if required.

A TS Gateway server is a type of gateway that enables authorized users to connect to remote computers on a corporate network from any computer with an Internet connection. A TS Gateway server enables Remote Desktop connections to a corporate network from the Internet without having to set up virtual private network (VPN) connections. Ask your network administrator whether you need to specify an TS Gateway server.

° User Name—Enter a user name for the connection.
° Password—Enter the password.
° Domain—Enter the domain name.

The User name, Password, and Domain name fields are optional. If you leave any of these fields blank, interactive login is required (users must enter the information at login time).

Options tab

The following figure shows the Options tab.
Use the following guidelines on the Options tab:

- **Wallpaper**—When selected, disables the desktop wallpaper.
- **Menu / Window animation**—When selected, disables the menu or window animation.
- **Theme**—When selected, disables the desktop themes.
- **Show content when dragging**—By default, when you "grab" a Window by the title bar and move it around, the contents of the window will move with it. Select this to disable this content view so that only the outline of the window moves when dragging it, until you drop the window. This option can be beneficial, because it uses less processing power.
- **Font smoothing**—Converts vector text to bitmap for better display.
- **Auto-connect to local devices**—Select any options (Printers, Serials, USB, Smart Cards, Sound, and Disks) to have the zero client automatically connect to the devices (USB—Redirects locally attached USB devices on the zero client to a Microsoft Windows terminal server. When the user connects to the terminal server, locally attached USB devices on the zero client are accessible).
- **RDP Audio Playback and RDP Audio Recording**—Select the audio options you want.

**Note**
The RDP Audio options enable the Cisco VXC client to transfer audio information. However, restrictions can still apply from the central server. Users should check with their system administrator to find out if two-way audio is supported in their Cisco VXC architecture.

- **Turn compression off**—When selected, turns compression off (intended for high-speed connections).
- **Optimize for low speed link**—When selected, allows optimization for low-speed connections, such as reducing audio quality or decreasing protocol-specific cache size. Intended for a connection spanning a WAN link or using dialup.
• Auto detect network - When selected, turns on the auto detect network feature. This feature is enabled by default. It also disables the Optimize for low speed link option and the Desktop Experience options by default.

• Mouse queue timer—Specifies the default queue timer of a mouse event in an ICA or RDP session (in 1/100 of a second). It can be used to adjust the bandwidth of a network