APPENDIX C

Upgrading Cisco VXC Manager Agents

This appendix contains advanced information about upgrading Cisco VXC Manager Agents (HAgent). It also provides information on Cisco VXC Manager Agent error codes.

Note Because the Cisco VXC 2000 Series devices use a Cisco VXC Manager Agent that is integrated into the firmware, the upgrade procedures in this appendix do not apply to these devices. These procedures are only applicable to the Cisco VXC 6215, and only if an updated Cisco VXC Manager Agent is released for the device.

The Cisco VXC Manager Agent is a small Web agent that runs within the operating system of the device being managed. It has a very small footprint and is optimized for the thin client environment. The Cisco VXC Manager Agent works with the Cisco VXC Manager Services on the Cisco VXC Manager Server to perform the actions that are needed by you, the administrator. The Cisco VXC Manager Agent interprets the commands sent by the Cisco VXC Manager Server and makes the necessary changes to the device being managed. In addition, the Cisco VXC Manager Agent also provides status updates about the device to the Cisco VXC Manager Server.

t includes:

Using the Auto-Agent Upgrade Feature

The Auto-Agent Upgrade feature enables existing versions of the Cisco VXC Manager Agent on a device to be upgraded automatically. With this preference enabled, a device is automatically upgraded to the most current version of the Cisco VXC Manager Agent when the device is discovered (or checks-in).

Caution In cases where you have FTP or HTTP limitations, or have a large number of devices with older Cisco VXC Manager Agents on your network, this operation could take a significant amount of time. Therefore, it is recommended that you begin upgrading older Cisco VXC Manager Agents selectively. After upgrading a number of the devices selectively, you can turn on the Auto-Agent Upgrade feature to complete the upgrading process, and to continue upgrading any new devices that are added to the network as Cisco VXC Manager discovers them.

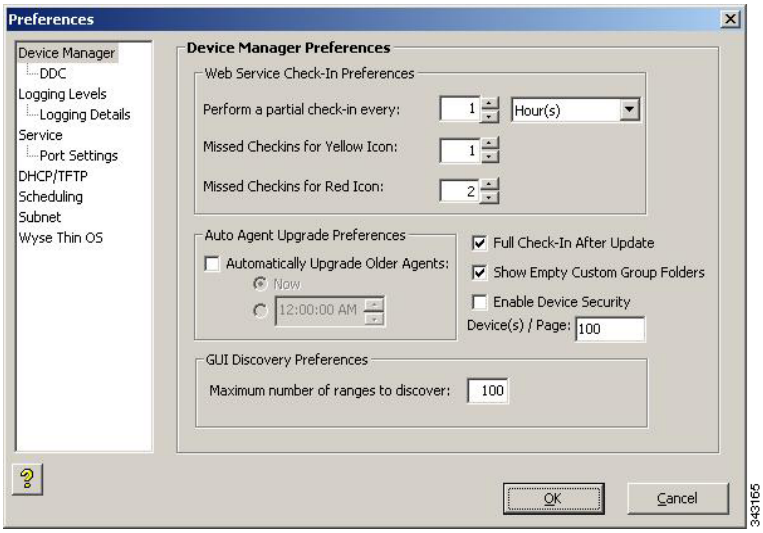
To enable automatic upgrading of Cisco VXC Manager Agents:

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager** and click **Preferences**.

Step 2 Double-click **Device Manager Preferences** to open the Preferences dialog box.

Figure C-1 Preferences—Device Manager



Step 3 Check the **Automatically Upgrade Older Agents** check box, and set the Auto-Agent Upgrade Preferences you want (selecting **Now** starts the upgrading process immediately; selecting the clock option allows you to set the desired time to start the upgrading process—a recommended time is during low network activity).

Tip By default, the time zone specified is the Database Update Server time zone (to specify a different the time zone, refer to Scheduling Preferences, page 7-70).

Be aware of the following:

- The new packages installed with Cisco VXC Manager are designed to upgrade existing Cisco VXC Manager Agent devices.
- Cisco VXC Manager Agent upgrades use the first 3 digits of the version number to determine if a newer Cisco VXC Manager Agent is available. The last digit is specific to Cisco VXC Manager for internal control and is not used by Auto-Agent Upgrade.
- If any Default Device Configuration (DDC) exists with Enforce Sequence enabled, Auto-Agent Upgrade will trigger the DDC to re-image devices, which will trigger Auto-Agent Upgrade in an infinite regression. Rebuild existing DDCs with an image containing the newest Cisco VXC Manager Agent.

Step 4 After you have finished your settings, click **OK**.

Tip For information on editing or deleting a scheduled update, see Managing the Schedules for Device Updates, page 5-21.

Understanding Cisco VXC Manager Agent Error Codes

This section contains information on the following errors:

- File Transfer Protocol Error Codes—The File Transfer Protocol (FTP) is a protocol that is able to transfer files between machines with different operating systems. The FTP utility issues an error, or reply, code to every user command. FTP errors are discussed in File Transfer Protocol (FTP) Error Codes, page C-3.
- Windows Sockets Error Codes—When using any TCP/IP application, it is possible for errors to occur in both configuration and networking. Many applications do not report these errors, but simply tell you that you have a network error. A list of possible errors (as reported by Microsoft) is shown in Windows Sockets Error Codes, page C-6.

File Transfer Protocol (FTP) Error Codes

The following are excerpts from RFC 959 for FTP.

An FTP reply consists of a three-digit number (transmitted as three alphanumeric characters) followed by some text. The number is intended for use by automata to determine what state to enter next; the text is intended for the human user.

The three digits of the reply each have a special significance. This is intended to allow a range of very simple to very sophisticated responses by the user-process. The first digit denotes whether the response is good, bad or incomplete. An unsophisticated user-process will be able to determine its next action (proceed as planned, redo, retrench, and so on) by simply examining this first digit. A user-process that wants to know approximately what kind of error occurred (for example, file system error, command syntax error) may examine the second digit, reserving the third digit for the finest gradation of information.

First Digit

There are five values for the first digit of the reply code:

- 1yz Positive Preliminary reply—The requested action is being initiated; expect another reply before proceeding with a new command (the user-process sending another command before the completion reply would be in violation of protocol; but server-FTP processes should queue any commands that arrive while a preceding command is in progress). This type of reply can be used to indicate that the command was accepted and the user-process can now pay attention to the data connections, for implementations where simultaneous monitoring is difficult. The server-FTP process can send at most, one 1yz reply per command.
- 2yz Positive Completion reply—The requested action has been successfully completed. A new request can be initiated.
- 3yz Positive Intermediate reply—The command has been accepted, but the requested action is being held in abeyance, pending receipt of further information. The user should send another command specifying this information. This reply is used in command sequence groups.

- 4yz Transient Negative Completion reply—The command was not accepted and the requested action did not take place, but the error condition is temporary and the action may be requested again. The user should return to the beginning of the command sequence, if any. It is difficult to assign a meaning to transient, particularly when two distinct sites (Server- and User-processes) have to agree on the interpretation. Each reply in the 4yz category might have a slightly different time value, but the intent is that the user-process is encouraged to try again. A rule of thumb in determining if a reply fits into the 4yz or the 5yz (Permanent Negative) category is that replies are 4yz if the commands can be repeated without any change in command form or in properties of the User or Server (for example, the command is spelled the same with the same arguments used; the user does not change his file access or user name; the server does not put up a new implementation).
- 5yz Permanent Negative Completion reply—The command was not accepted and the requested action did not take place. The User-process is discouraged from repeating the exact request (in the same sequence). Even some permanent error conditions can be corrected, so the human user may want to direct his User-process to re-initiate the command sequence by direct action at some point in the future (for example, after the spelling has been changed, or the user has altered his directory status).

Second digit (Function Groupings)

The following function groupings are encoded in the second digit:

- x0z Syntax—These replies refer to syntax errors, syntactically correct commands that do not fit any functional category, non-implemented or superfluous commands.
- x1z Information—These are replies to requests for information, such as status or help.
- x2z Connections—Replies referring to the control and data connections.
- x3z Authentication and accounting—Replies for the login process and accounting procedures.
- x4z—Unspecified as yet.
- x5z File system—These replies indicate the status of the Server file system through the requested transfer or other file system action.

Third Digit

The third digit gives a finer gradation of meaning in each of the function categories specified by the second digit, as shown in the following list:

Tip The text associated with each reply is recommended, rather than mandatory, and may even change according to the command with which it is associated. The reply codes, on the other hand, must strictly follow the specifications in the last section; that is, Server implementations should not invent new codes for situations that are only slightly different from the ones described here, but rather should adapt codes already defined.

- **100**
  - 110 Restart marker reply.
  - 120 Service ready in minutes.
  - 125 Data connection already open; transfer starting.
  - 150 File status okay; about to open data connection.
- **200**
  - 200 Command okay.

  - 202 Command not implemented, superfluous at this site.
  - 211 System status, or system help reply.
  - 212 Directory status.
  - 213 File status.
  - 214 Help message.
  - 215 NAME system type.
  - 220 Service ready for new user.
  - 221 Service closing control connection. Logged out if appropriate.
  - 225 Data connection open; no transfer in progress.
  - 226 Closing data connection. Requested file action successful (for example, file transfer or file abort).
  - 227 Entering Passive Mode (h1, h2, h3, h4, p1, p2).
  - 230 User logged in, proceed.
  - 250 Requested file action okay, completed.
  - 257 PATHNAME created.
- **300**
  - 331 User name okay, need password.
  - 332 Need account for login.
  - 350 Requested file action pending further information.
- **400**
  - 421 Service not available, closing control connection. This may be a reply to any command if the service knows it must shut down.
  - 425 Can't open data connection.
  - 426 Connection closed; transfer aborted.
  - 450 Requested file action not taken. File unavailable (for example, file busy).
  - 451 Requested action aborted: local error in processing.
  - 452 Requested action not taken. Insufficient storage space in system.
- **500**
  - 500 Syntax error, command unrecognized. This may include errors such as command line too long.
  - 501 Syntax error in parameters or arguments
  - 502 Command not implemented.
  - 503 Bad sequence of commands.
  - 504 Command not implemented for that parameter.
  - 530 Not logged in.
  - 532 Need account for storing files.
  - 550 Requested action not taken. File unavailable (for example, file not found, or no access).
  - 551 Requested action aborted: page type unknown.

- 552 Requested file action aborted. Exceeded storage allocation (for current directory or data set).
- 553 Requested action not taken. File name not allowed.

Windows Sockets Error Codes

WINSOCK Errors are generated when a script is running on a Cisco VXC Manager Agent. In such a case, the Cisco VXC Manager Agent either had trouble obtaining or sending a file as part of the script. The following is a list of possible errors (as reported by Microsoft):

Tip Errors are listed in alphabetical order by error macro. Some error codes defined in Winsock2.h are not returned from any function—these are not included in this list:

- WSAEINTR 10004—Interrupted function call. A blocking operation was interrupted by a call.
- WSAEACCES 10013—Permission denied. An attempt was made to access a socket in a forbidden way.
- WSAEFAULT 10014—Bad address. The system detected an invalid pointer address.
- WSAEINVAL 10022—Invalid argument. Some invalid argument was supplied.
- WSAEMFILE 10024—Too many open files. Too many open sockets.
- WSAEWOULDBLOCK 10035—Resource temporarily unavailable. Socket operation not available at this time.
- WSAEINPROGRESS 10036—Operation now in progress. A blocking operation is currently executing.
- WSAEALREADY 10037—Operation already in progress. An operation was attempted on a non-blocking socket with an operation already in progress.
- WSAENOTSOCK 10038—Socket operation on non-socket. An operation was attempted on something that is not a socket.
- WSAEDESTADDRREQ 10039—Destination address required. A required address was omitted from an operation.
- WSAEMSGSIZE 10040—Message too long. A message sent on a datagram socket was larger than the internal message buffer.
- WSAEPROTOTYPE 10041—Protocol wrong type for socket. A protocol was specified in the socket function call that is not supported.
- WSAENOPROTOOPT 10042—Bad protocol option. An unknown, invalid or unsupported call was made.
- WSAEPROTONOSUPPORT 10043—Protocol not supported. The requested protocol has not been configured into the system.
- WSAESOCKTNOSUPPORT 10044—Socket type not supported. The support for the specified socket type does not exist.
- WSAEOPNOTSUPP 10045—Operation not supported. The attempted operation is not supported.
- WSAEPFNOSUPPORT 10046—Protocol family not supported. The protocol family has not been configured into the system or no implementation for it exists.

- WSAEAFNOSUPPORT 10047—Address family not supported. An address incompatible with the requested protocol was used.
- WSAEADDRINUSE 10048—Address already in use. An application attempts to bind a socket to an IP address/port that has already been used for an existing socket.
- WSAEADDRNOTAVAIL 10049—Cannot assign requested address. The requested address is not valid.
- WSAENETDOWN 10050—Network is down. A socket operation encountered a dead network.
- WSAENETUNREACH 10051—Network is unreachable. A socket operation was attempted to an unreachable network.
- WSAENETRESET 10052—Network dropped connection. The connection has been broken due to keep-alive activity detecting a failure while the operation was in progress.
- WSAECONNABORTED 10053—Software caused connection abort. A connection was aborted by the software in your machine, possibly due to a TCP/IP configuration error, data transmission time-out or protocol error.
- WSAECONNRESET 10054—Connection reset by peer. An existing connection was forcibly closed by the remote host.
- WSAENOBUFS 10055—No buffer space available. An operation on a socket could not be performed because the system lacked sufficient buffer space or because a queue was full.
- WSAEISCONN 10056—Socket is already connected. A connect request was made on an already-connected socket.
- WSAENOTCONN 10057—Socket is not connected. A request to send or receive data was disallowed because the socket is not connected.
- WSAESHUTDOWN 10058—Cannot send after socket shutdown. A request to send or receive data was disallowed because the socket had already been shut down.
- WSAETIMEDOUT 10060—Connection timed out. A connection did not properly respond after a period of time.
- WSAECONNREFUSED 10061—Connection refused. No connection could be made because the target machine actively refused it.
- WSAEHOSTDOWN 10064—Host is down. A socket operation failed because the destination host is down.
- WSAEHOSTUNREACH 10065—No route to host. A socket operation was attempted to an unreachable host.
- WSAEPROCLIM 10067—Too many processes. A Windows Sockets implementation may have a limit on the number of applications that can use it simultaneously.
- WSASYSNOTREADY 10091—Network subsystem is unavailable. This error is returned if the sockets implementation cannot function because the system is currently unavailable.
- WSAVERNOTSUPPORTED 10092—Winsock.dll version out of range. The current Windows Sockets implementation does not support the Windows Sockets specification version requested.
- WSANOTINITIALISED 10093—Startup failed. The application socket startup failed.
- WSAEDISCON 10101—Graceful shutdown in progress. Returned to indicate that the remote party has initiated a graceful shutdown.
- WSATYPE_NOT_FOUND 10109—Class type not found. The specified class was not found.
- WSAHOST_NOT_FOUND 11001—Host not found. No such host is known.

- WSATRY_AGAIN 11002—Non-authoritative host not found. A temporary error during host name resolution and means that the local server did not receive a response from an authoritative server.
- WSANO_RECOVERY 11003—This is a nonrecoverable error. A nonrecoverable error occurred during a database lookup.
- WSANO_DATA 11004—Valid name, no data record of requested type. The requested name is valid and was found in the database, but does not have the correct associated data being resolved for it.
- ERROR_INTERNET_TIMEOUT 12002—Internet time-out. The request has timed out.