WTOS – FTP/HTTP/HTTPS/CCM UPGRADE METHODS

A Technote by Customer Support

July 2014

Knowledge Base Solution #

10566

TABLE OF CONTENTS

Table of Contents **1**
Summary **4**
Audience **4**
Affected Products **4**
Requirements **5**
Windows PC or Server with IIS and FTP Services installed. 5
Access to the required firmware from Wyse. 5
If using CCM 5
IMPORTANT 5
Procedure for FTP Upgrades **5**
1 . Create the Directory Structure. 5
2 . Get the Firmware. 5
3 . Backup Your INI File. 6
4 . Edit or Create the WNOS.INI File. 6
5 . Prepare the Thin Client. 7
6 . Define the File Server - Manually. 7
7 . Define the File Server – Using DHCP 7
8 . Verify the Upgrade. 8
9 . Reboot the Thin Client. 8
10 . Verify the Upgrade. 8
11 . Restoring the WNOS.INI File to Production. 8
Procedure for HTTP/HTTPS Upgrades **9**
1 . Setup the File Types. 9
2 . Create the Directory Structure. 9
3 . Get the Firmware. 9
4 . Define the File Server - Manually. 10
5 . Define the File Server – Using DHCP 10
Procedure for CCM Upgrades **11**
1. Get the Firmware 11
2. Add the File to the Inventory 11

3. Verify Uploaded File 12
4. Set the Advanced Options, Modify and Apply the Policy 12

Table 1 - Firmware File Names for the different WTOS-based Clients 6
Table 2 - Option Tags 162 and 162 Information 10

SUMMARY

This document will show you how to properly configure and setup an FTP/HTTP/HTTPS Windows server to upgrade your WTOS-based thin clients and also how to properly setup CCM to upgrade the firmware. If you are using an FTP/HTTP/HTTPS server other than Microsoft IIS, use these instructions as a reference, however, please note that we cannot provide support for anything other than IIS and Microsoft DHCP server.

AUDIENCE

Customers, 1st Level Support, and Systems Engineering Group

AFFECTED PRODUCTS

All thin clients using Dell Wyse ThinOS Version Release 7 and Release 8. (Referred here as R7 and R8)

REQUIREMENTS

Windows PC or Server with IIS and FTP Services installed.

If you don't have the FTP server installed, you can go to the Microsoft Knowledge Base (http://support.microsoft.com/search/) and search for documents "How to setup an FTP server" or "How to setup an HTTPS server". You can specify your OS to reduce the number of articles.

Access to the required firmware from Wyse.

Please note that Wyse ThinOS (WTOS) thin clients require that you be enrolled in our Software Maintenance Program to be eligible to receive new versions of WTOS software and subsequent releases of corresponding documentation distributed via our Self-Service Portal at https://support.wyse.com/OA_HTML/ibuhpage.jsp .

If using CCM

The client connection to the CCM service should be set before going over this process. Setting up CCM is not covered in this article.

IMPORTANT

To avoid unforeseeable issues, please ensure that when you upgrade your firmware, you DO NOT skip versions. E.G. from version 7.0 you upgrade to 7.1. From 7.1 you upgrade to 8.0, etc. You should not go directly from firmware version 7.0 to 8.0.

PROCEDURE FOR FTP UPGRADES

1 . Create the Directory Structure.

Installing the Windows IIS creates the directory **C:\inetpub\ftproot** (which is known as the FTP ROOT). Under this folder you will need to create another folder name ***\wyse*** and under ***\wyse*** create another folder and name it ***\wnos***. By now you should have a directory structure that reads:

C:\inetpub\ftproot\wyse\wnos

2 . Get the Firmware.

The firmware files provided by Wyse, normally come in the form of a compressed self-extracting (.EXE) or Zipped (.ZIP) file. The firmware files must be extracted from those files and placed in the ***\wnos*** folder (See table 1 for File Names in relation to your specific model.)

Please note that the "BOOT" file is only required for manufacturing purposes and is not always present). Verify that the file ***wnos.ini*** exist in the **\wnos** directory. If this file does not exist, you must create it using a text editor. See

Table 1 for the file names used on the different models. Note: the D10D, 5212 and Z10D use the same firmware file.

Model	File Name
3110-C10LE	C10_WNOS C10_BOOT **
5012-D10D	ZD10_WNOS
5012-D10DP	PD10_WNOS
R10L + (EOL)	R10_WNOS R10_BOOT **
S10 * + (EOL)	RCA _WNOS RCA_BOOT **

Model	File Name
3010-T10	DOVE_BOOT
3012-T10D	T10D_BIOS ** T10D_WNOS
V10L/LE + (EOL)	VL10_WNOS VL10_BOOT **
7012-Z10D	ZD10_WNOS
5212 (AIO)	ZD10_WNOS

TABLE 1 - FIRMWARE FILE NAMES FOR THE DIFFERENT WTOS-BASED CLIENTS

Notes:

* ***The S10 will not support WTOS 8.***

***** With the exception of the T10, BOOT or BIOS files are not always required or included with an upgrade. Always install BOOT and BIOS files if included with the distribution file.***

+ End of Life devices are not tested with the latest released firmware. Their mention on this document is for your reference and does not imply any functionality or deviation from the EOL policy..

3 . Backup Your INI File.

If you already have a WNOS.INI file, make a backup copy before you continue.

4 . Edit or Create the WNOS.INI File.

Open (or create) the ***wnos.ini*** file with a **text editor**, and enter (or modify) the following three lines and then save the file.

Autoload=2
Signon=0
FactoryDefault=Yes

This tells the thin client to upgrade the firmware with the firmware installed on the server only if the firmware on the thin client is older than the version on the server, there is no need to login to do this and to reset the client back factory defaults.

5 . Prepare the Thin Client.

For R7 and R8 – Select the Configuration Icon, expand the "Central Configuration: option and select the "General" Tab.

6 . Define the File Server - Manually.

R7 and R8 – Go to the "General" tab (See Figure 1 for R7 and Figure 2 for R8).

The **File Servers/Path** field should have the IP Address of the FTP Server/ Directory (change to the correct values if necessary).

i.e.: 192.257.1.201/wyse

Note: The starting path must be ***/wyse***

The "**Username**" field should have "**Anonymous**" and the "**Password**" field's password is already set (DO NOT CHANGE).

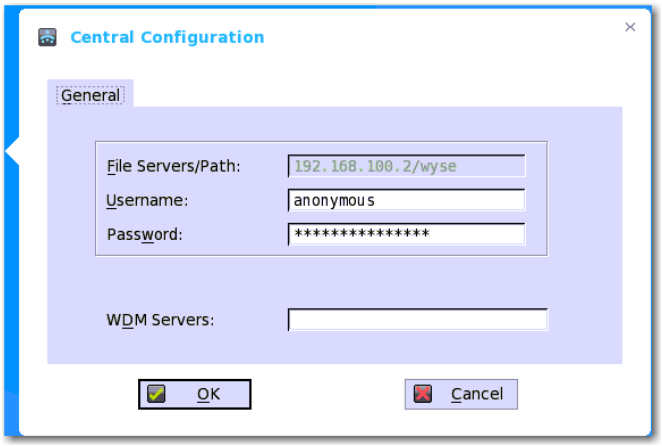

FIGURE 1 - VERSION 7.X THIN CLIENT

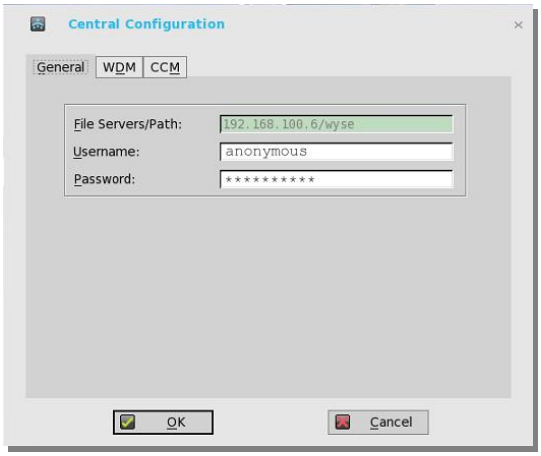

Figure 2 - Version 8.x Thin Client

Note: If there is no default password or if the password has been changed, then you'll have to set it to something in an email format (i.e. ***abe@abc.com***) or set the thin client back to factory defaults. This will put the Anonymous user back in with the default password but you'll have to reconfigure the thin client.

7 . Define the File Server – Using DHCP

The Second method uses DHCP option tags 161 and 162 to hand the WTOS thin client the File Server and Path information. You will need to create these options on your DHCP server, configure them with the correct server information and enable the on the DHCP server Scope you will be using in your environment. See Table 2 for more information on setting these options.

8 . Verify the Upgrade.

To check if the thin client upgraded at the end of this process, click on the "Desktop" button and select "System Information". Under the "General" tab, Note the "System Version", and verify that the client was upgraded.

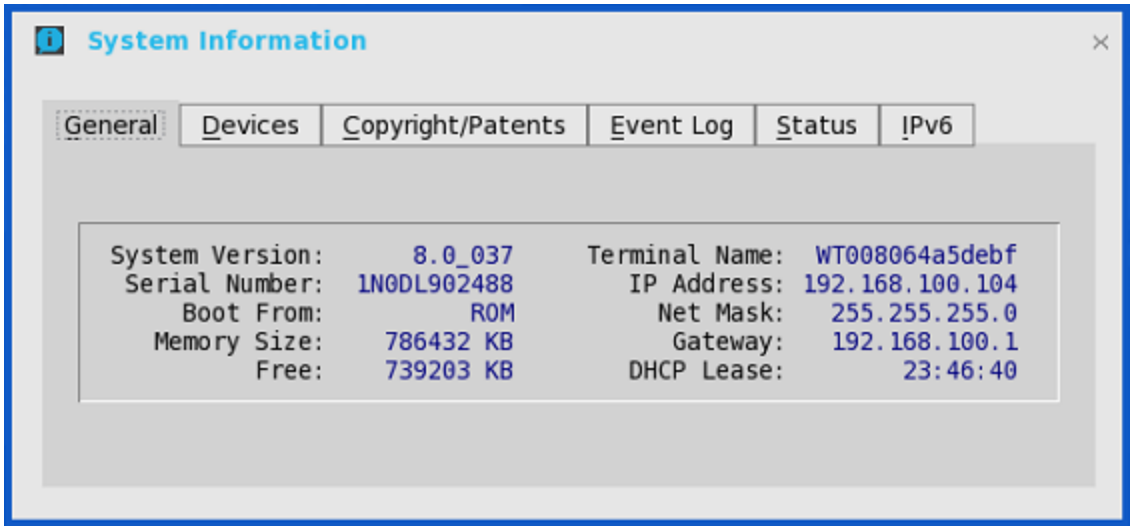

FIGURE 3 - SYSTEM INFORMATION SCREEN

9 . Reboot the Thin Client.

Restart the thin client and you should see a small progress bar go across the screen and load the new image on the thin client.

10 . Verify the Upgrade.

To verify that the thin client was upgraded, click on the "Desktop" button and select "System Information". Under the "General" tab, Note the "System Version". It should now be different than the version on step 8.

11 . Restoring the WNOS.INI File to Production.

You can return your WNOS.INI file back to its original state.

PROCEDURE FOR HTTP/HTTPS UPGRADES

If you require HTTP or HTTPS support, please follow these steps"

1 . Setup the File Types.

Verify that the web server can identify the files types used by WTOS. We need to create two MIME types under IIS. The MIME's option needs to be configured on a per site basis. On a default IIS install:

a. Launch the IIS admin console.

b. Browse to the **Default Web Site**, right click and select **Properties**.

c. Choose the **HTTP Headers** tab and under the **MIME Map** section choose **File Types** then **New Type**.

d. Add the two MIME types as shown below. Use ".**INI**" and "**.**" for the **associated extension** fields.

e. Apply the settings and close the IIS admin console.

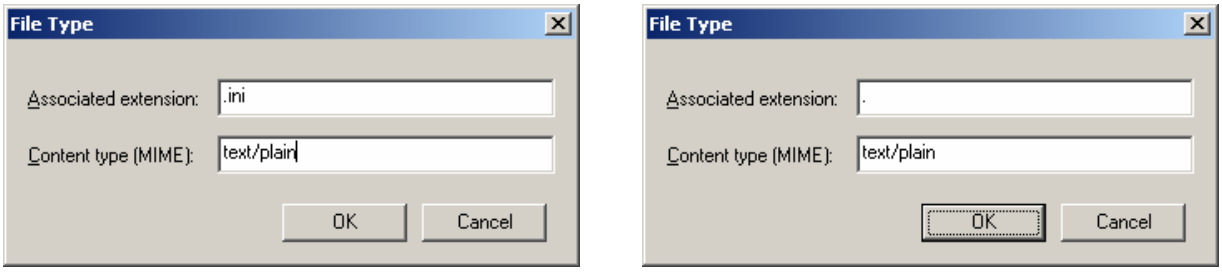

Figure 4 - Adding MIME Types

2 . Create the Directory Structure.

Installing IIS creates the default directory C:\inetpub\WWWroot. Under this folder please create the following directory structure.

C:\inetpub\wwwroot\wyse\wnos

3 . Get the Firmware.

Place the WTOS firmware and .INI files in the \WNOS directory.

- More information can be located in the WTOS Administrator's Guide along with sample .INI files. For both resources please visit the Wyse Customer Support Knowledgebase and click on Reference Guides.

4 . Define the File Server - Manually.

There are two types of methods which can be used to assign the WTOS thin computing device to the correct HTTPS server initially. First, you can manually enter the File Server and Path on the WTOS device by click on Desktop - System Setup - Network - File Servers/Path and entering the following information.

Example: *https:///IPADDRESS/wyse*

5 . Define the File Server – Using DHCP

The Second method uses DHCP option tags 161 and 162 to hand the WTOS thin client the File Server and Path information. You will need to create these options on your DHCP server, configure them with the correct server information and enable the on the DHCP server Scope you will be using in your environment. See figure 5 and Figure 6 for an example of what these options look like.

Option Tag #	Description	Type	Comments
161	File Server Address	String	Can be either the name or the IP address of the file server. If a name is given, the name must be resolvable by the DNS server(s) specified in Option 6. If the option provided by the server is blank or the server provides no value for the field, the machine on which the DHCP server resides is assumed to also be the file server.
162	Root path to the file server	String	If the option provided by the server is blank and the server provides no value for the field, a null string is used. \wyse\wnos is automatically appended to the search path. For example, if you enter Pub\serversoftware, the path searched will be *pub|serversoftware|wyse|wnos.* **Note:** You can have the \wyse automatic component of the search path omitted by appending a dollar sign ($) to the entered path. For example, if you enter pub\serversoftware$, the path searched will be *pub|serversoftware|wnos.* **Note:** The usage or omission of a leading slash (\) on the path is critical on some servers. Some servers limit access to the root path of the user specified at login. For those servers, the usage of the leading slash is optional.

TABLE 2 - OPTION TAGS 162 AND 162 INFORMATION

Specific information on how to setup 161 and 162 tags is located in the Wyse Thin OS Administrators guide available in the Wyse Customer Support Knowledgebase and click on Reference Guides.

NOTE: For more information on the directory structure and DHCP Options Tags required, please review the information available in the Wyse ThinOS Administrators Guide and the Wyse ThinOS INI Reference Guide appropriate for your firmware version.

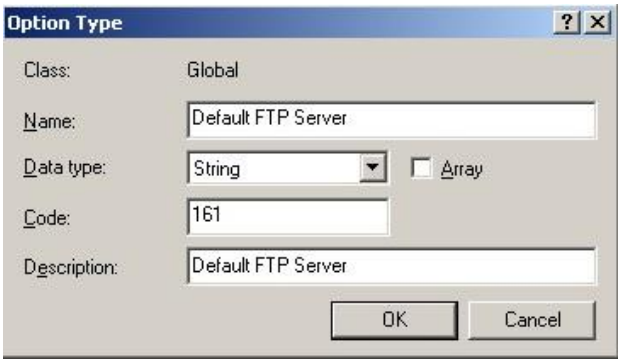

FIGURE 5 - EXAMPLE FOR DHCP OPTION TAG 161

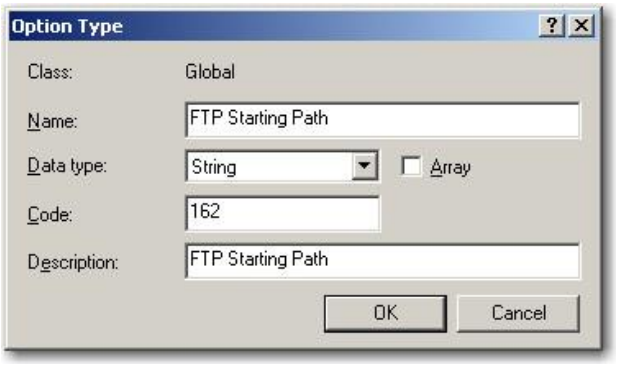

FIGURE 6 - EXAMPLE FOR DHCP OPTION TAG 162

PROCEDURE FOR CCM UPGRADES

This procedure will not cover the installation and setup of CCM, only how to use CCM to upgrade your WTOS-based thin client.

1. **Get the Firmware**

   The firmware files provided by Dell Wyse, normally come in the form of a compressed self-extracting (.EXE) or a compressed Zipped (.ZIP) file. The firmware files must be extracted from those files and placed in a location where you can access them from the computer you will be using to access the CCM console.

2. **Add the File to the Inventory**

   Once you have the file available (extracted and copied on your computer) , go to the CCM Console

   - Select the App & Data tab
   - Select the "Inventory" button on the left pane
   - Click on the "Add File" Button (Figure 7). This will open the dialog box which will allow you to use the "Browse" button to navigate to the location of the file.
   - Select the file
   - Set the "Type" to "Firmware"

- Enter a description of the file that will help you identify the file later. See Figure 8.

  Example: T10D Firmware file version 2.0_214HF

- Press "Upload" to complete this step.

HINT: you can check the box labeled "Override existing file" if you make a mistake on the type or you want to change the description of the file.

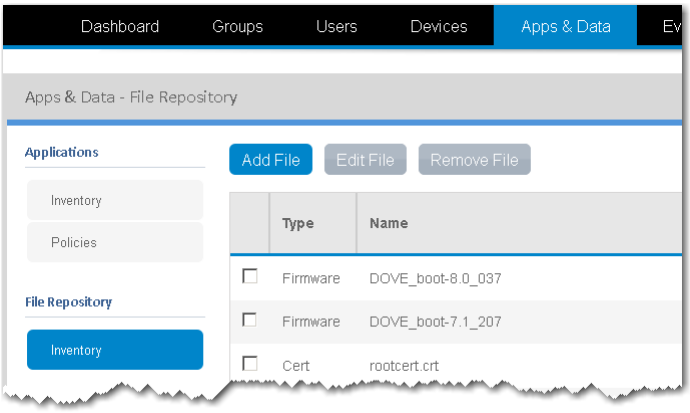

FIGURE 7 - ADDING A FILE TO INVENTORY

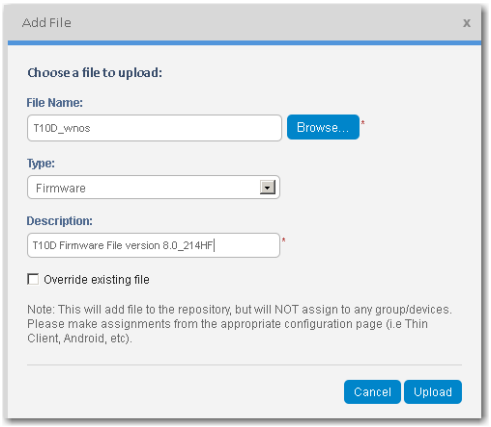

FIGURE 8 - SELECTING FILE TO ADD

3. Verify Uploaded File

It is always a good idea to insure that the file was uploaded and that you can identify it. Take a look at Figure 9 and compare it with what you entered on Figure 8. CCM automatically adds the firmware version to the end of the file name you uploaded, which makes it easier to identify.

FIGURE 9 - UPLOADED FILE

4. Set the Advanced Options, Modify and Apply the Policy

In order to allow the firmware to be installed on your thin client, you need to make some changes to the policy. To do this, click on the "Groups" tab and find the Policy Group that includes your thin client and click on the "Edit Policies > ThinOS/Xenith" option. On the left pane under ThinOS/Xenith Settings, select the "Advanced" button. In "Line 1" (See Figure 10) enter the following:

FactoryDefault=Yes

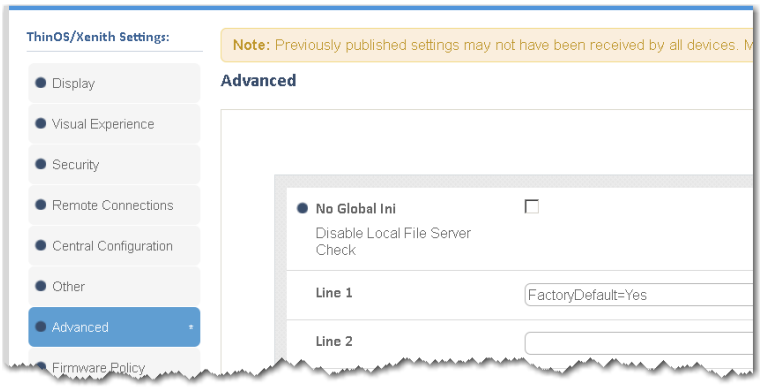

FIGURE 10 - ADVANCED OPTIONS

Once completed, go to the left pane under ThinOS/Xenith Settings, select the "Firmware Policy" button and do the following"

- Verify that the **Disable Live Upgrade** option is "Checked". This will prevent you from upgrading (meaning re-booting) the devices right after you press the "Save & Publish" button.

  WARNING: Leaving this option unchecked may cause a mayor disruption to your operation if done during business hours.

- Set the **Firmware Update Logic** to the desired value.
  - Do not update – Does not make any changes
  - New firmware only – Will only upgrade the firmware **(recommended)**
  - Any different firmware – Will upgrade or downgrade the firmware on the thin client. Some thin clients require a minimum version to operate, a setting them up to a lower version may damage it.
- Verify that the **Skip local Firmware Check** option is checked. This will prevent the client from executing any "autoload=" parameter that may be set in the WNOS.INI.
  - **HINT**: You may also want to make sure that under the "Advanced" button the option **No Global Ini** is checked
- From the dropdown menu, select the **Platform Type** (Device Model) and the **Firmware to auto-deploy** dropdown box, select the file you uploaded. See Figure 10.

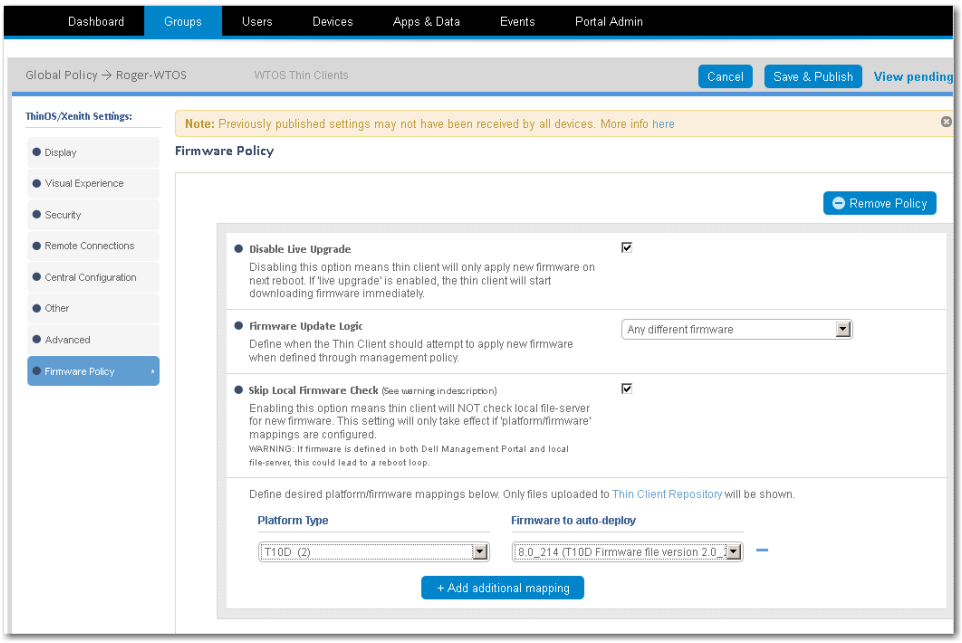

FIGURE 11 - FIRMWARE POLICY

- If you wish to add more devices, click on the "**+ Add additional mapping**" and repeat the previous step for the new Platform Type.
- Press the **Save & Publish** button to apply the policy. Your devices will now be upgraded according to your settings:
  - If **Disable Live Upgrade** is left un-checked – Your thin clients will reboot immediately after pressing the "Save & Publish" button.
  - If **Disable Live Upgrade** is checked – Your thin clients will be upgraded after the next reboot.

You setup is now complete.