config@WEB S02 Initial Install

SAGE1-SFT-S0220 V2.0

Proprietary and Confidential to Schneider Electric

Schneider Electric North America Headquarters
1415 South Roselle Road
Palatine, IL 60067

Phone: 1-847-397-2600
Fax: 1-847-925-7500

Schneider Electric
14400 Hollister St., Suite #400
Houston, TX 77066-5706

Phone: 1-713-920-6800
Fax: 1-713-920-6909
E-mail: SAGERTU_Support@schneider-electric.com

config@WEB S02 Initial Install

For Reference Only

© Copyright 2015 by Schneider Electric

The information contained in this document is confidential and proprietary to Schneider Electric . It is not to be copied or disclosed for any purpose except as specifically authorized in writing by Schneider Electric . Although the information contained herein was correct and verified at the time of publication, it is subject to change without notice.

Manual No. SAGE1-SFT-S0220

Rev	Date	Description	Technical Review	Admin. Approval
0.0	29-May-2012	Created for Non-Secure to Secure Config@WEB Firmware Update.		
0.1	11-Jun-2012	RTU automatically reboots after install.		
0.2	20-Jun-2012	Updated for H1 version		
1.0	24-Jul-2012	Release	N/A	
1.1	16-Oct-2013	Updated for J0 version		
2.0	22-Oct-2015	Updated for K0 release		
			Garry Macejewski, Manager, RTU Engineering	Chris Kerr, Manager, RTU S/W Engineering

1.1 Introduction

This user manual describes the software operation and features of the Schneider Electric SAGE Remote In an effort to better serve our customers, we have simplified the process of upgrading the RTU (with its configuration) to the latest secure firmware in the C3414-500-S02K0 release. The procedure is: Start the Initial Installer, type in RTU IP and User credentials, hit Start, wait until prompted, reboot the RTU. If you have trouble, see Chapter 3: Troubleshooting.

This procedure is perfect for customers who are having trouble with the GUI in older firmware versions or would like to use the new features in the latest firmware.

Cyber security features are available to users, but no further action is required if the upgraded RTU is not included in the critical infrastructure guidelines. See the Documentation folder for instructions on generating user keys and SSL certificates and adding those to your configuration and users packages.

This document describes updating the SAGE RTU Firmware:

To: **C3414-500-S02K0**

From: **C3414-500-001YZ**

Hardware Versions:

SAGE 3030M	**SAGE 1430**
SAGE 2400	**SAGE 1410**
SAGE 1450	**LANDAC II**

The purpose of this procedure is to upgrade an existing C3414 CPU based SAGE RTU (3030M, 2400, 1450, 1430, 1410 or LANDAC II) from the C3414-500-001YZ baseline firmware to the C3414-500-S02K0 secure firmware.

Proprietary and Confidential to Schneider Electric

1.2 Procedure

1 Download the Secure Firmware Update Package from the customer exchange site (C3414-500-S02K0 Secure_Firmware_Zip_Package) available at:

https://infrastructurecommunity.schneider-electric.com/groups/rtu-downloads

2 You will have to sign up for an account and request membership to this group before downloading SAGE Firmware:

Getting the Latest SAGE Firmware

3 Extract the contents of the zip file to your PC. Due to enhanced permissions on Windows 7, you will probably have to extract it to your "My Documents" folder. You need to have write access to the extracted folder.

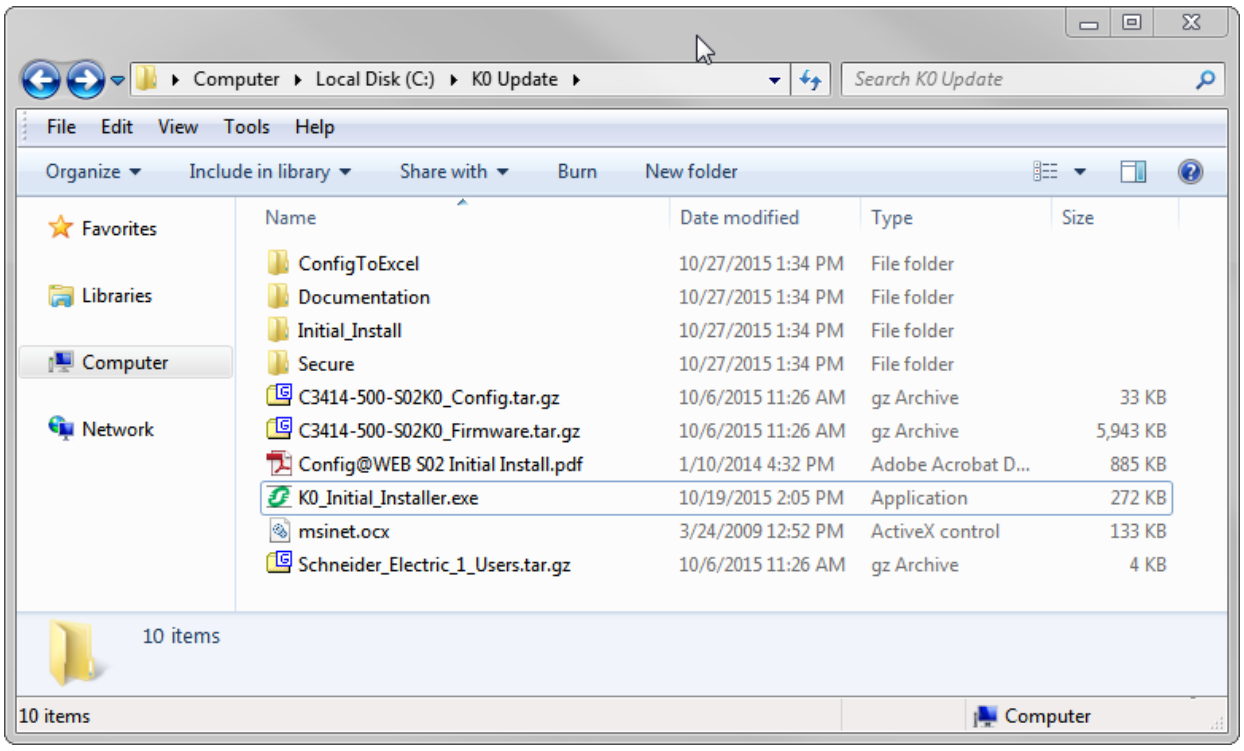


Figure 1: Secure Firmware Update Package

4 Start the XY_Initial_Installer.exe program to start the upgrade process.

5 Type in the IP Address, Username, and Password of the SAGE RTU you would like to convert to the Secure Firmware. Click Start Upgrade

SAGE Secure Firmware Initial Installer
Schneider Electric
RTU To Upgrade
RTU IP Address
172.18.150.50
Username
Admin
Password
Start Upgrade
Update Progress

6 The progress of the upgrade will be displayed in the Update Progress text box.

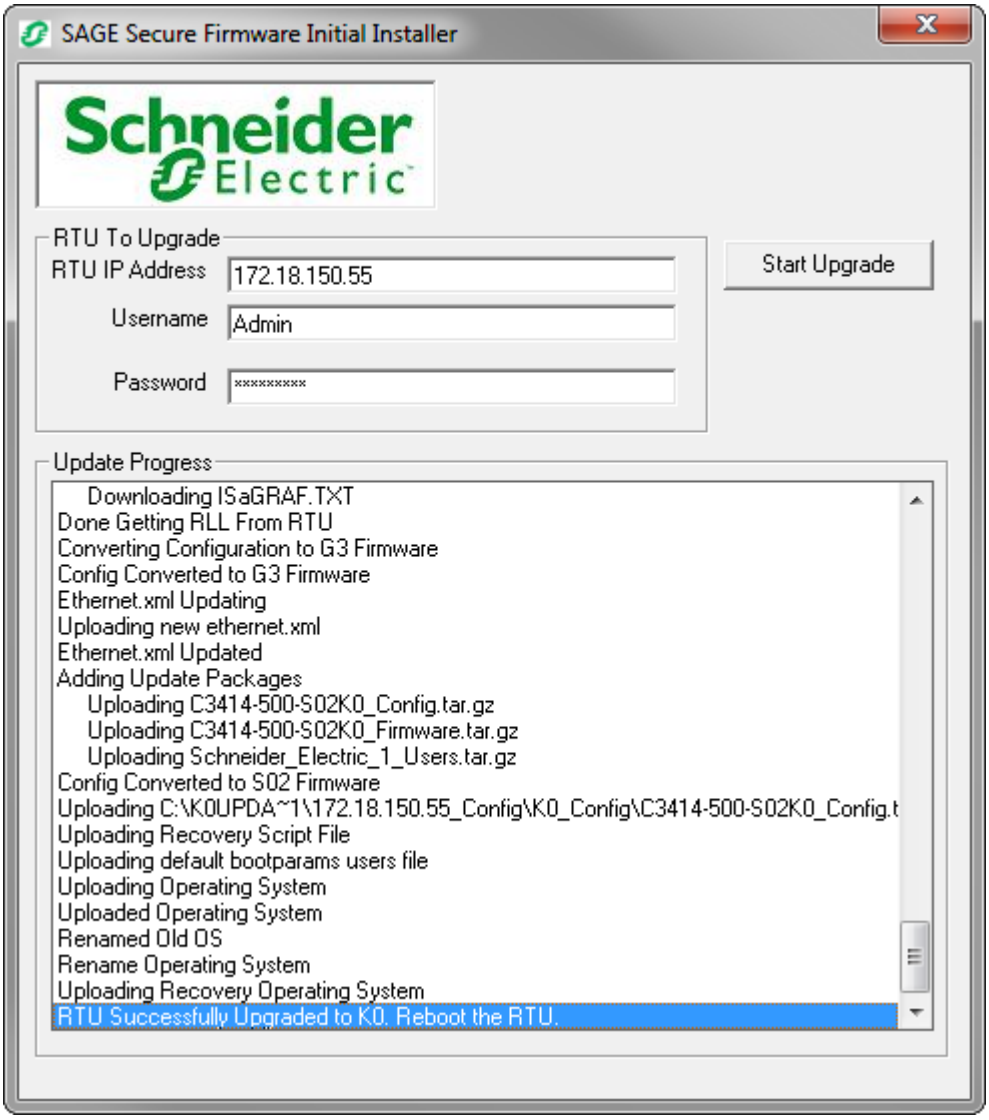


Figure 2: Initial Installer Progress

7 "RTU Successfully Upgraded to K0. Reboot the RTU." will be the last line.

8 Reboot the RTU.

9 The Secure Operating System provided with the C3414-500-S02YZ firmware will now automatically install the rest of the firmware and your RTU configuration to its proper location and reboot again on its own.

10 Your RTU will now be at the Secure Firmware version with your old configuration automatically updated and running in the RTU. The Username and Password are:

Username: Admin

Password: Telvent1!

Your RTU's configuration was converted to the new Secure Configuration (_Config.tar.gz) package format. It is stored in C:\K0_Initial_Install\'IP'_Config\K0_Config\C3414-500-S02K0_Config.tar.gz

We suggest that you backup the 'IP'_Config folder to a secure location for safe keeping.

See the new Config@WEB Secure Software manual for instructions on how to use the new features and tools included in the secure firmware. This is in the Documentation folder shown in Figure 1: Secure Firmware Update Package.

The C3414-500-001YZ configuration, templates, ISaGRAF, and bootline.xml file (which contains the IP address of the RTU) has been saved on the PC and upated to the C3414-500-001G3 firmware version needed for use with the new Configuration Conversion tool for the C3414-500-S02YZ firmware and stored in a folder named "C:\K0_Initial_Install\'IP'_Config" where 'IP' is the IP address of the RTU you are working with. See Figure 3: Configuration Backups

Caution: If you have RTUs with the same IP address, a new use of this procedure will overwrite an existing folder with the same name.

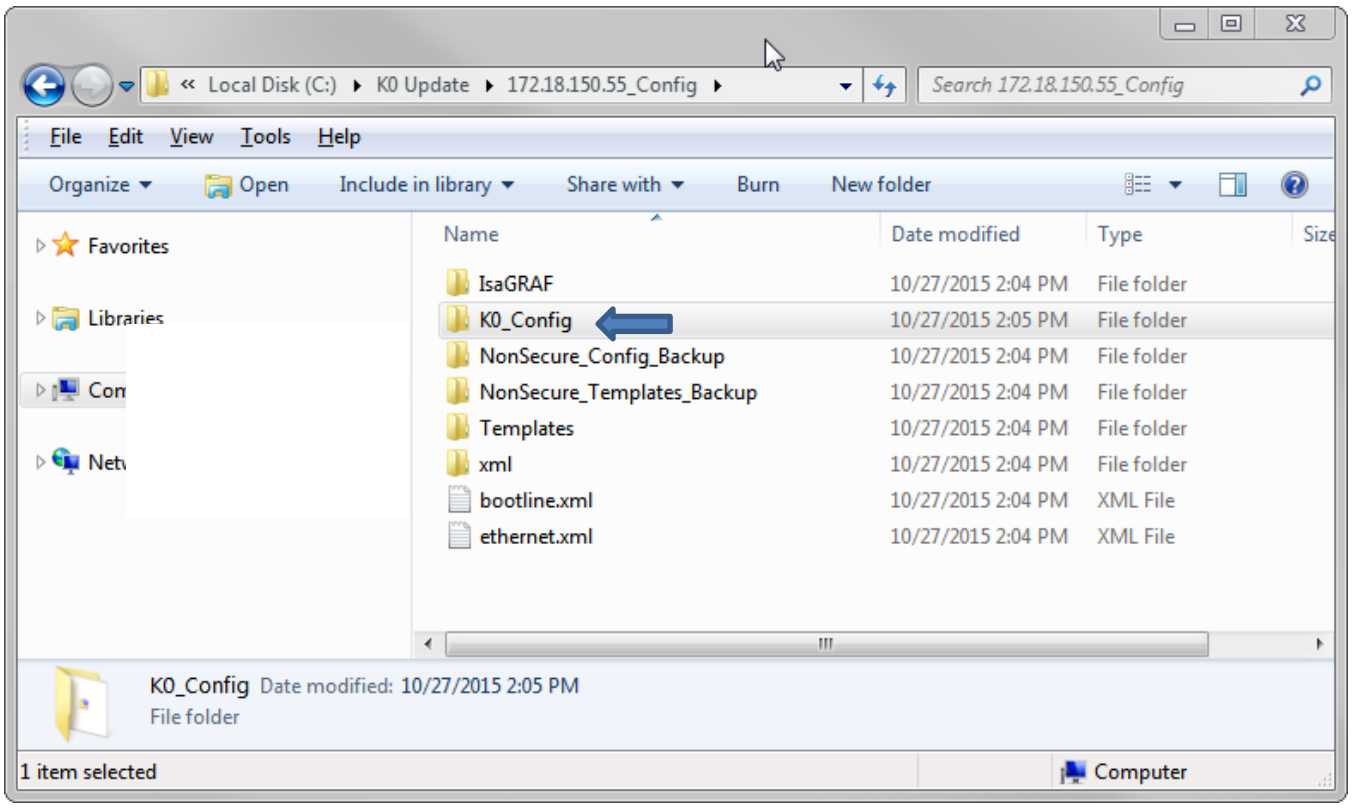


Figure 3: Configuration Backups

1.3 Troubleshooting

When updating the firmware, PC or network security may prevent the following tests from being completed successfully. If you are NOT successful in performing these tasks, the network or PC security settings will have to be modified to allow these tasks to be performed. Contact your Network or PC Administrator to change the network or PC settings to enable connectivity.

Before starting the upgrade, determine the account and password you will use to log into the RTU to upgrade the firmware. Using the account and password, verify access to your RTU by running the following tests.

If any of the tests using FTP fails, see Section 1.3 to the RTU such that FTP can be used to log in to the RTU. Contact your Network Administrator to change the network or PC settings to enable connectivity.

1.3 Extract the Zip File

You may see a message like, the following if you do not extract the contents of the .zip file to your hard drive before starting the installation process. Start the process again from Step 3.

Figure 4: Initial Installer Not Extracted from Zip File

1.3 Ping the RTU from the PC updating the firmware.

In a cmd window (or click start/click run/type “cmd<Enter>”)

Type “ping <IP Address of RTU><Enter>”.

Close command window – type “exit<Enter>”

If the ping test fails, correct the connection to the RTU such that the ping command executes correctly. Repeat this test until the RTU responds to the ping command.

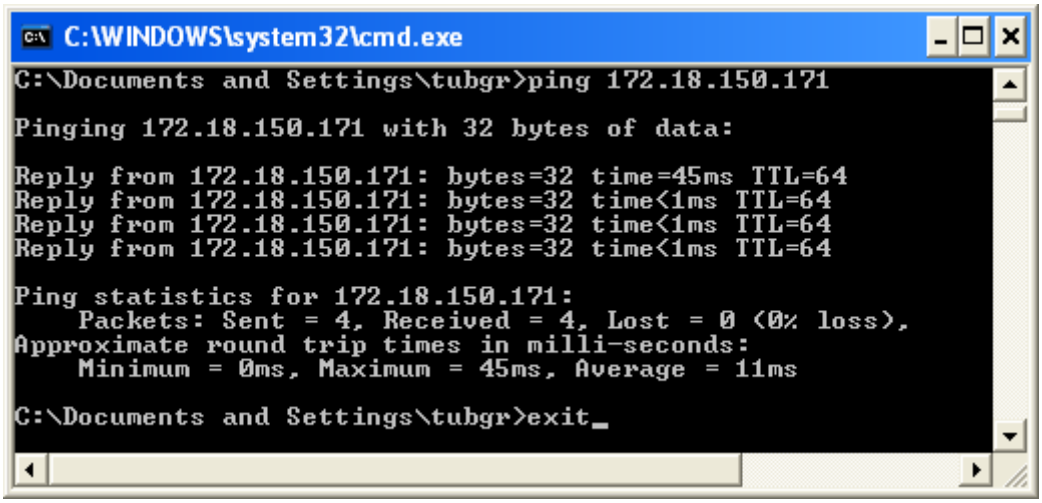


Figure 5: Ping the RTU

1.3 Log in and out of the RTU using telnet on the PC updating the firmware.

In a cmd window (or click start/click run/type “cmd<Enter>”)

Type “telnet <IP Address of RTU><Enter>”

You should receive a “->”prompt from the telnet server. If not, you must perform the upgrade locally or change settings on network security settings if connected over a network.

Type “version<Enter>”

You should see the version of VxWorks and the bootline, similar to the example below.

Type a “<Ctrl>d” to terminate the telnet session.

Close cmd by typing “exit<Enter>”.

If the login using telnet fails, correct the connection to the RTU such that telnet can be used to log in to the RTU. Repeat this test until you can successfully log in to the RTU.

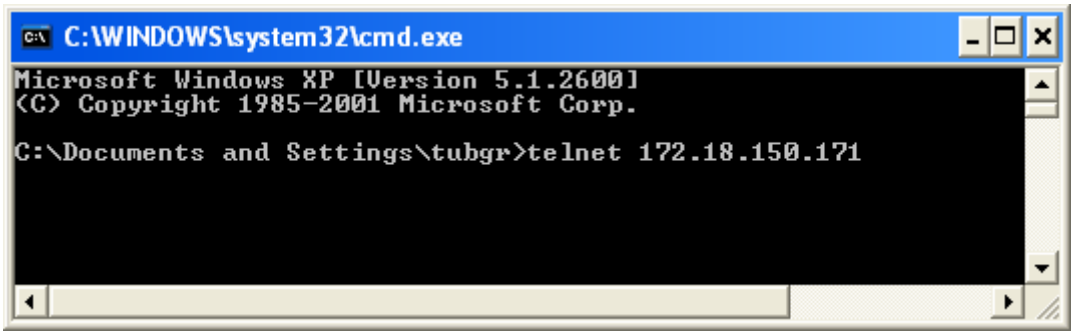


Figure 6: Telnet to the RTU

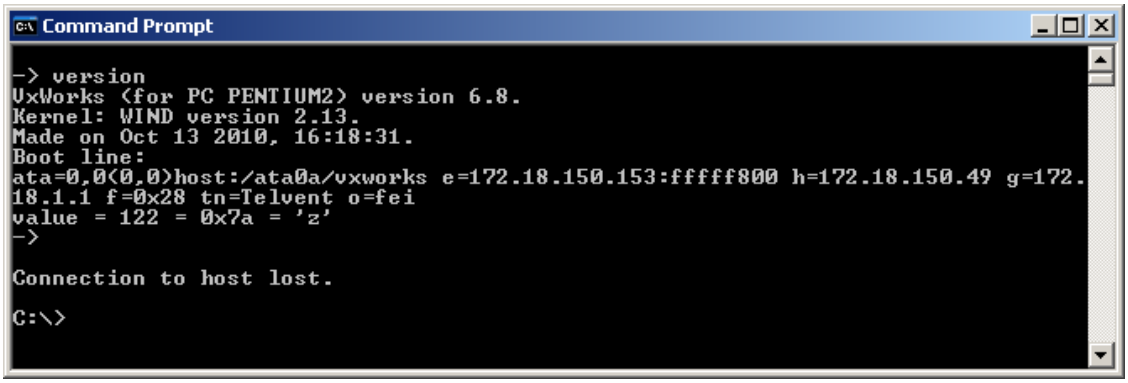


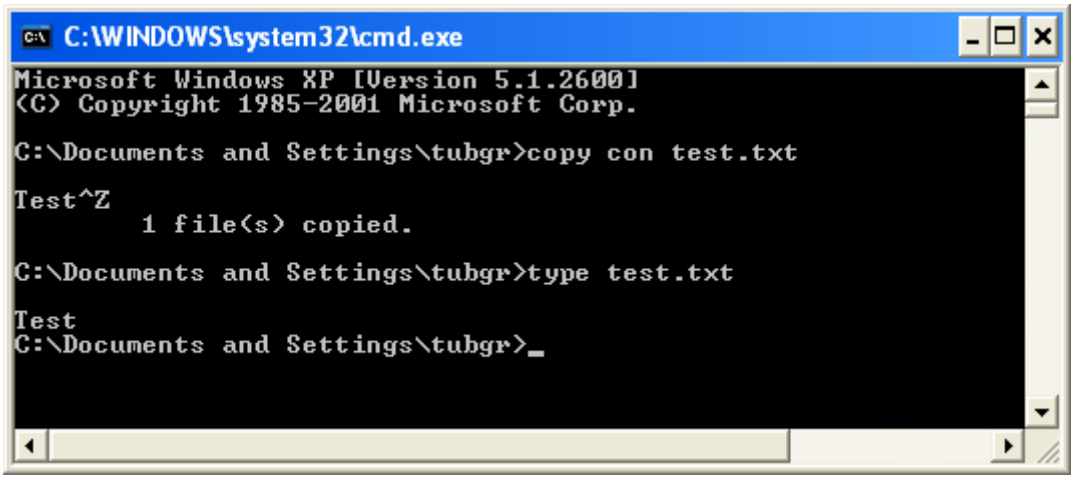
Figure 7: version Command

1.3 Get and Put files with FTP to the RTU

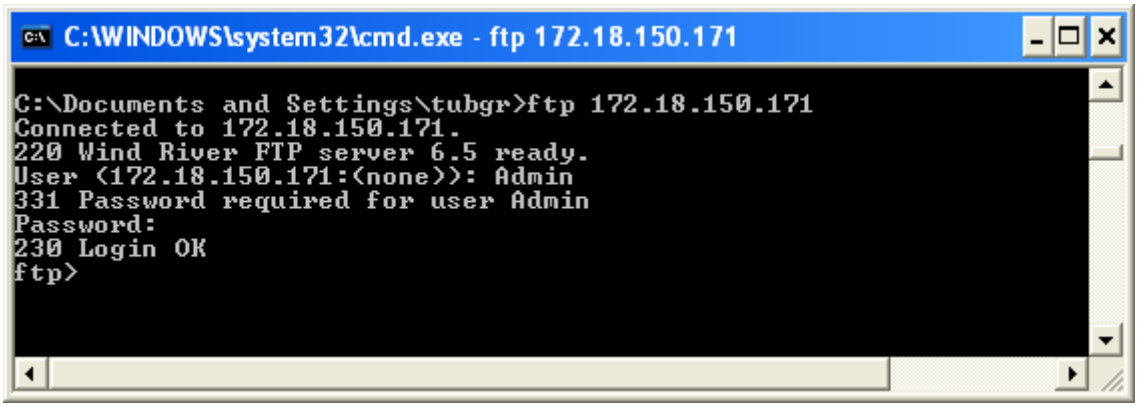
In a cmd window (or click start/click run/type “cmd<Enter>”)

Create a small text file to use to transfer, type “copy con test.txt<Enter>”
“Test^z<Enter>”. The ^z is “<Ctrl>z” (hold down <Ctrl> key and type z).

Verify the content of the file – type “type test.txt<Enter>”



Log onto the RTU using FTP with the account and password for the account you are going to use convert to the secure firmware. Type “ftp <IP Address of RTU><Enter>”, “<Account Name><Enter>", and “<Password><Enter>”.



Display the working directory – type “pwd<Enter>”.

Put onto the RTU the text file – type “put test.txt<Enter>”.

Verify the file was transferred – type “dir test.txt<Enter>”.

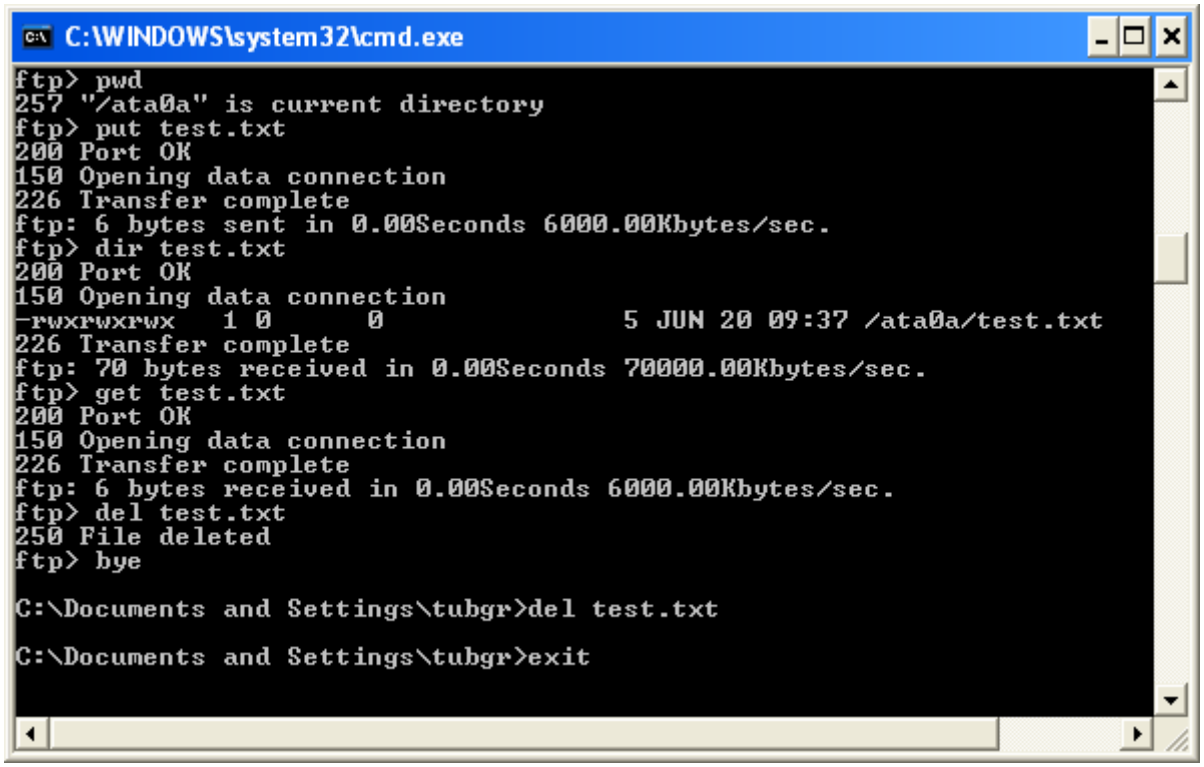
Get the same file – type “get test.txt<Enter>”.

Delete the file on the RTU – type “del test.txt<Enter>”.

Log out of FTP – type “bye<Enter>”.

Delete the file on your computer – type “del test.txt<Enter>”.

Close the cmd window – type “exit<Enter>”.



1.3 Firewall Settings

You might need to add this program to your Windows 7 Firewall settings to allow incoming FTP data to this application. If your computer is having trouble downloading the bootline.xml file from the RTU, you may need to do this. Your Network Admin may need to assist you.

Go to Start -> Search -> Firewall -> Allow a program or feature through Windows Firewall. This will probably have to be done by your PC or Network Administrator, depending on your corporate IT settings.

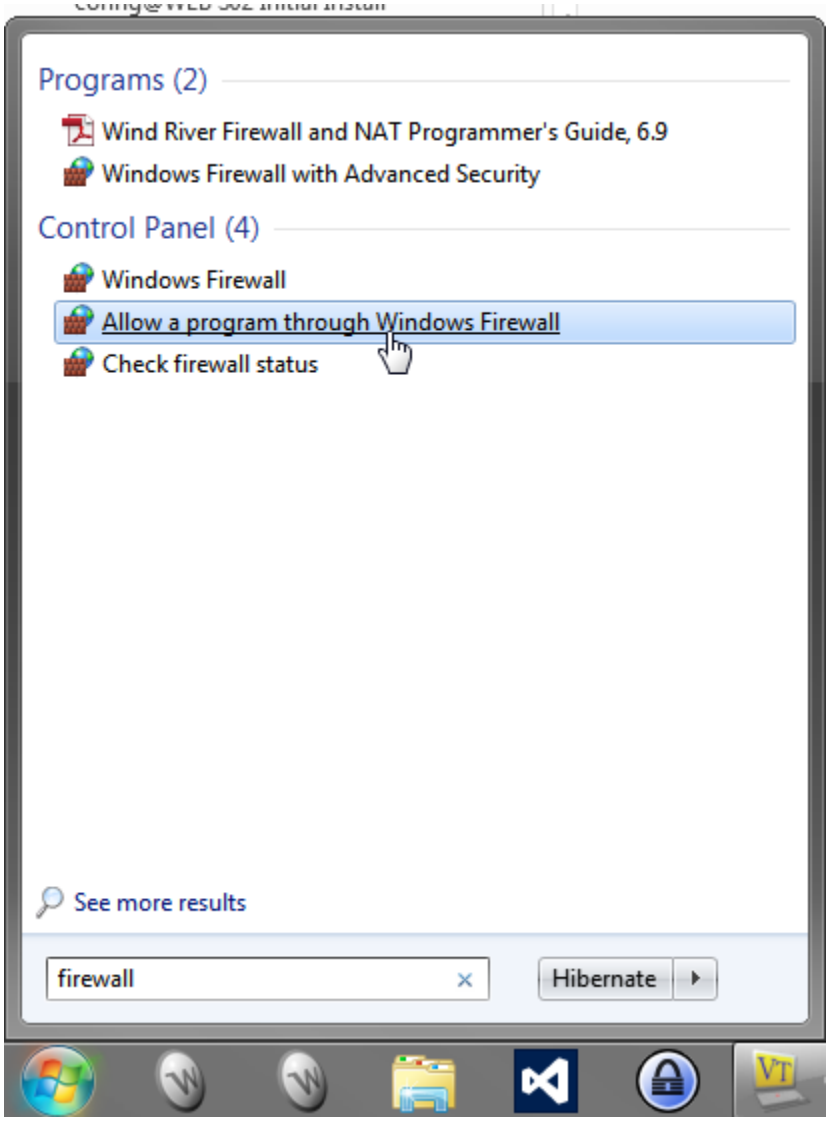


Figure 8: Allow a program through Windows Firewall

Optionally, you may disable Windows Firewall temporarily. If this is done, the following can be disregarded.

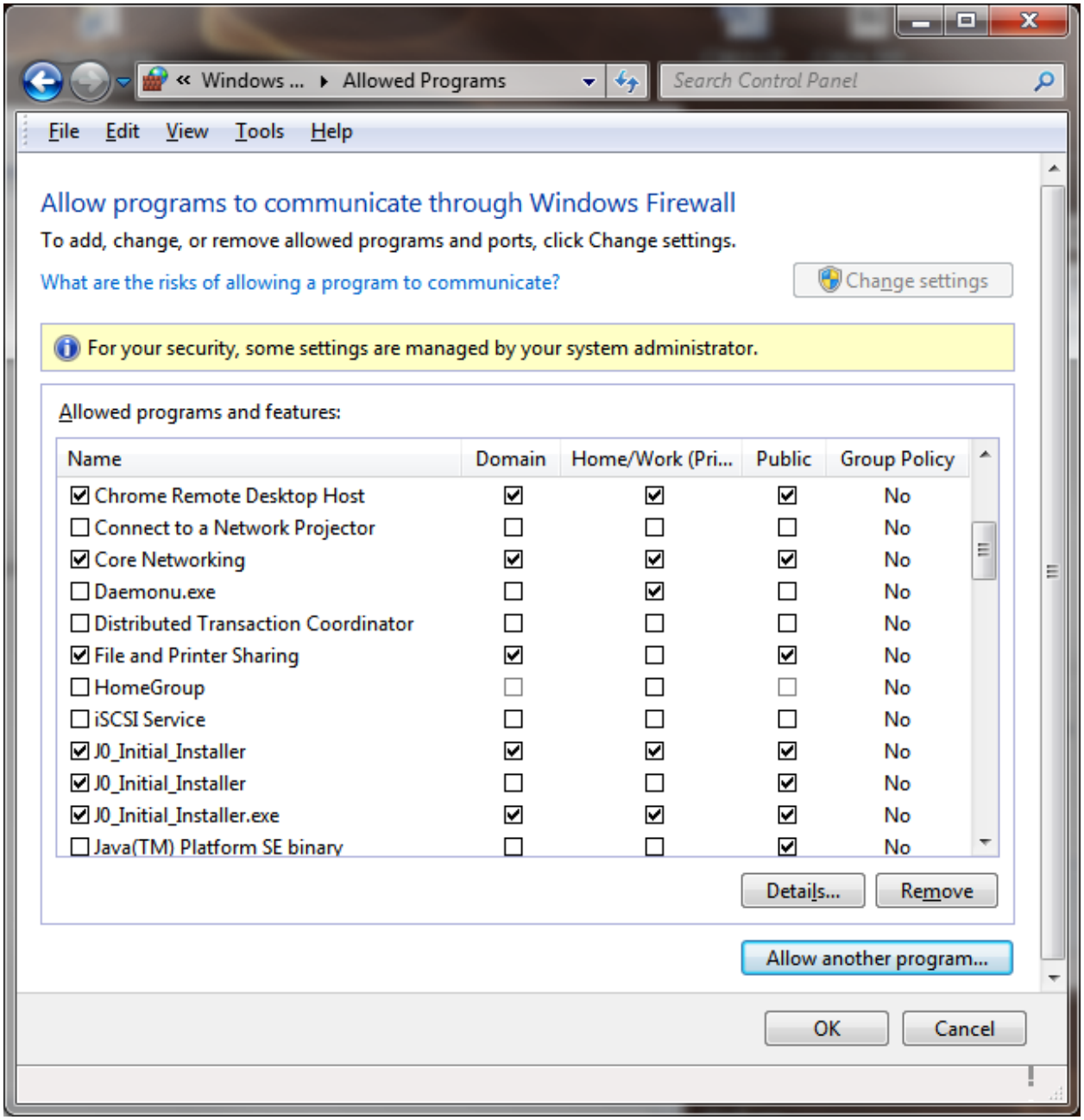


Figure 9: Windows Firewall Settings

Hit Allow another program…Browse to C:\K0_Update\K0_Initial_Installer.exe. Hit OK.

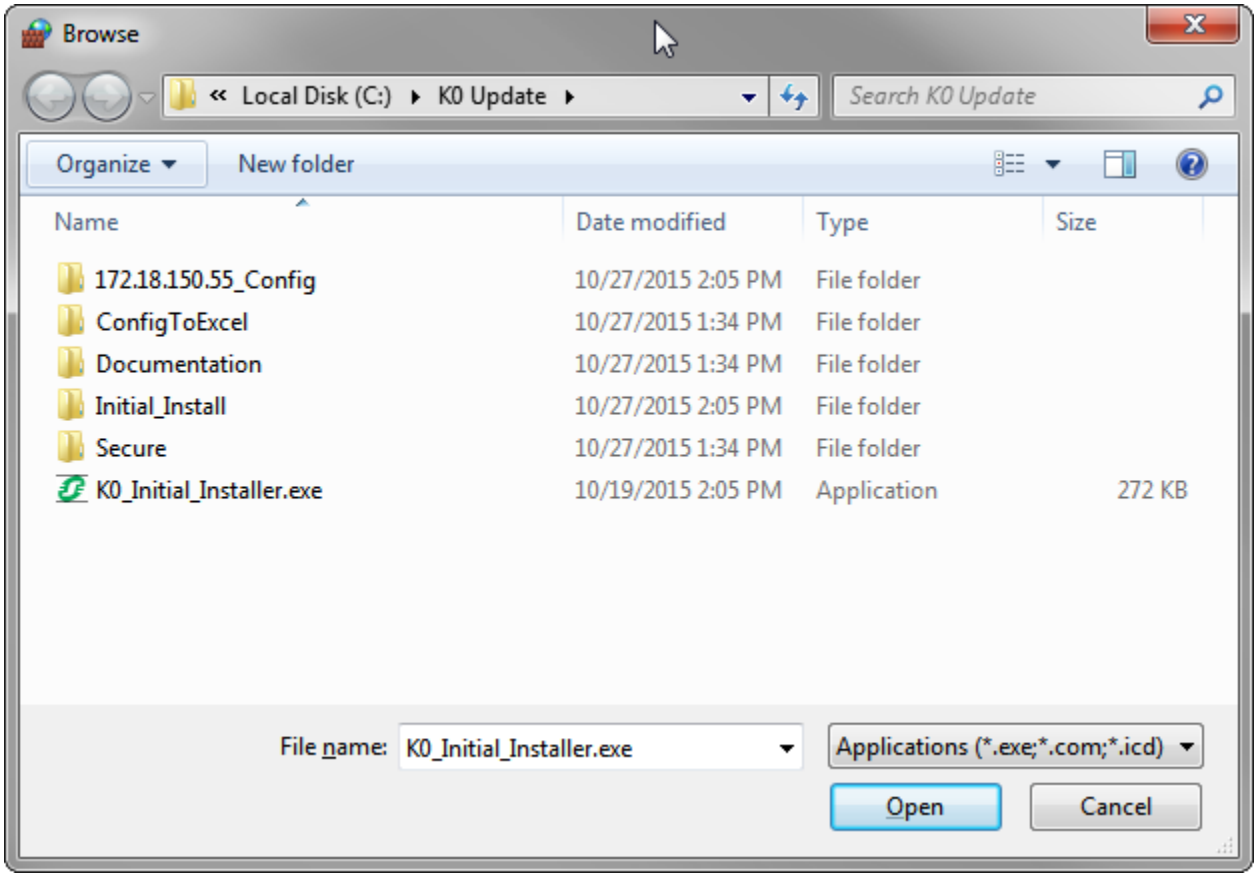


Figure 10: Browse to Initial Installer

Go back to the Control Panel -> Windows Firewall Settings Page as shown below.

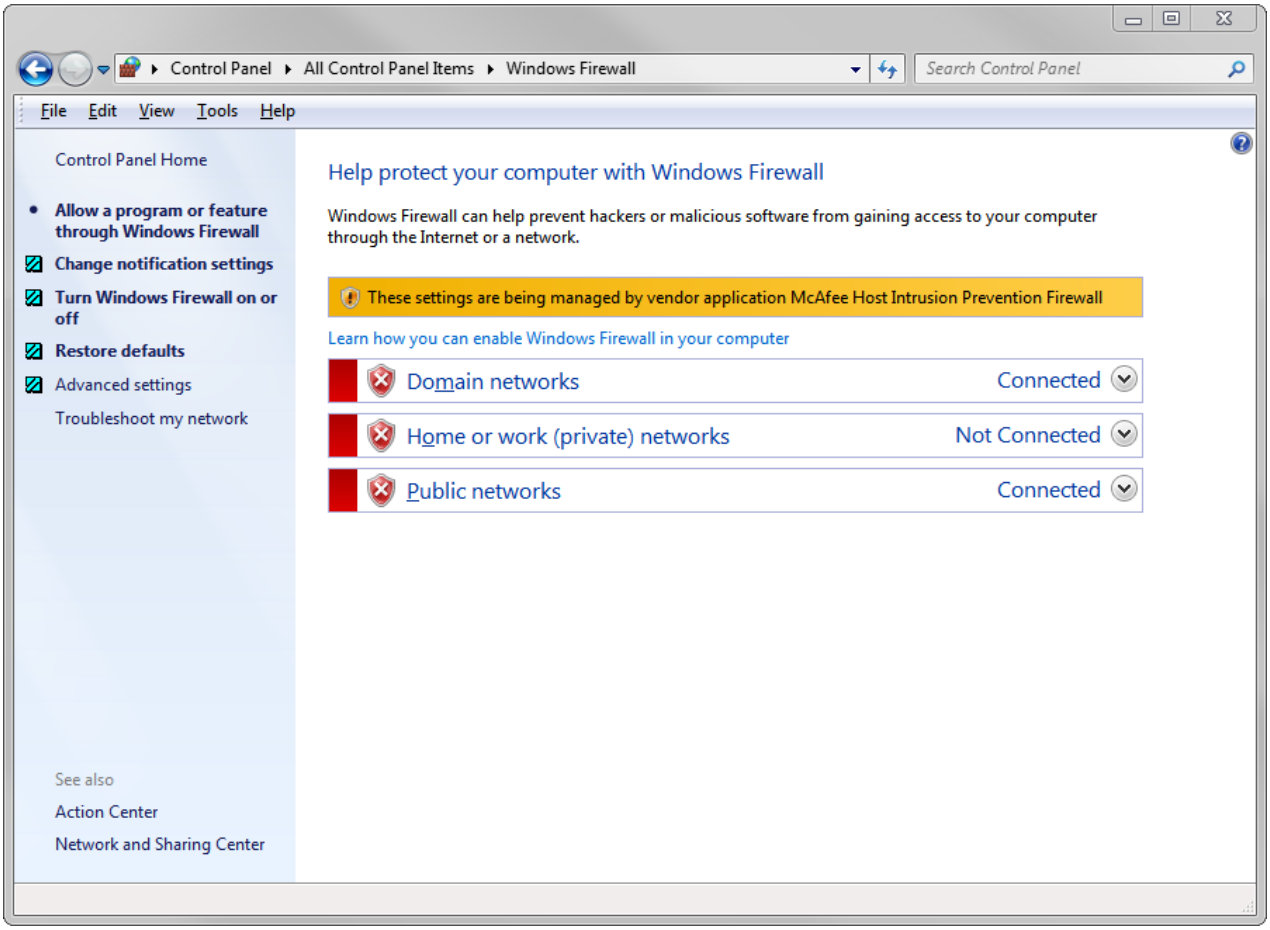
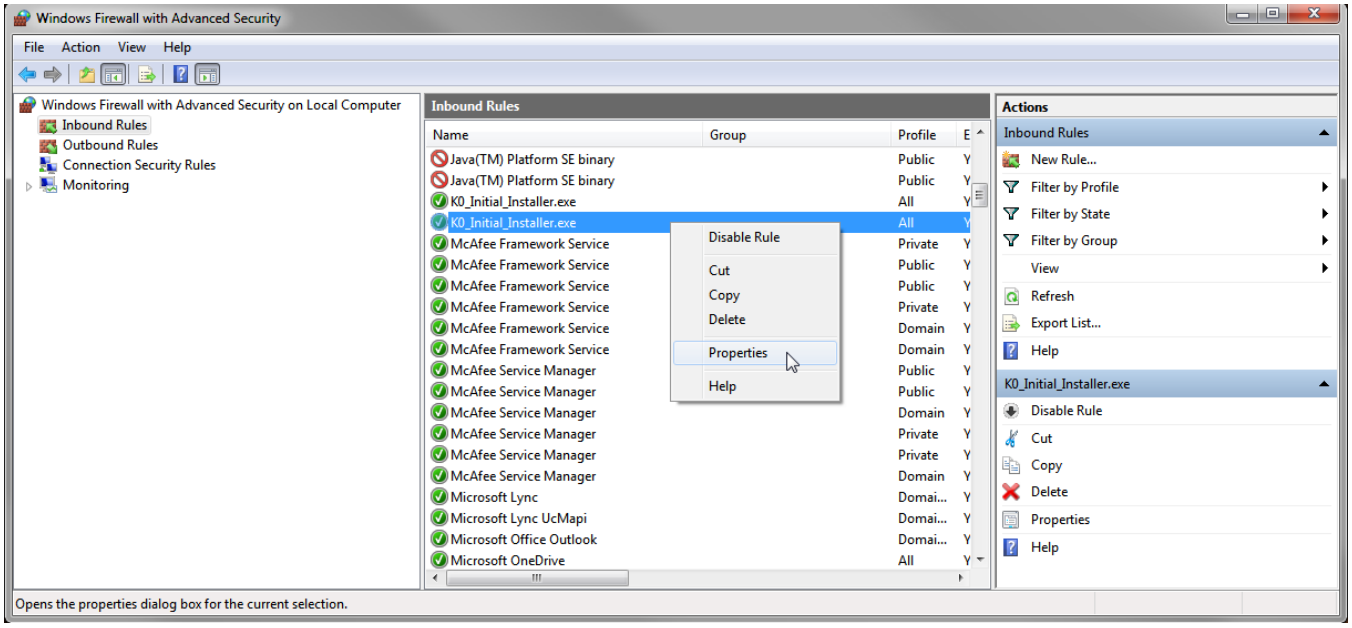
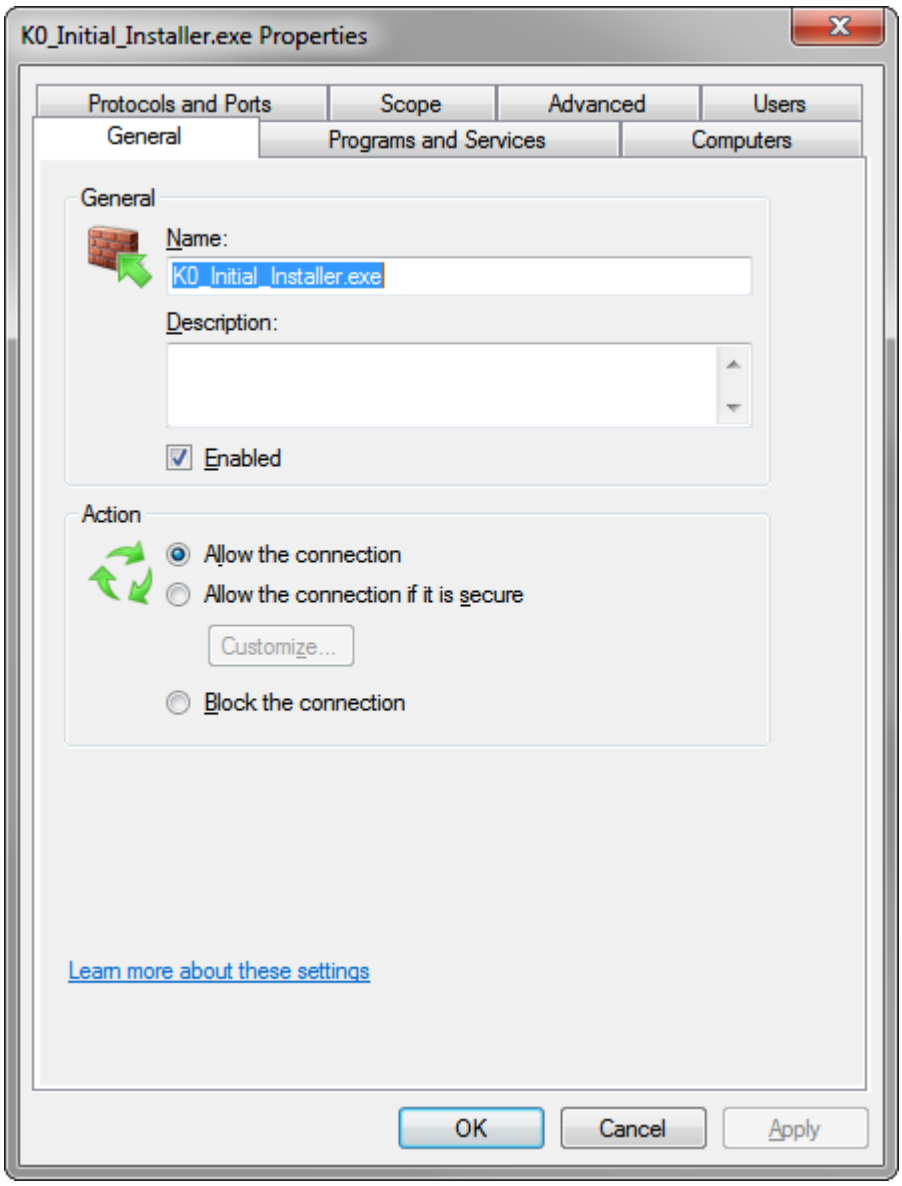


Figure 11: Windows Firewall

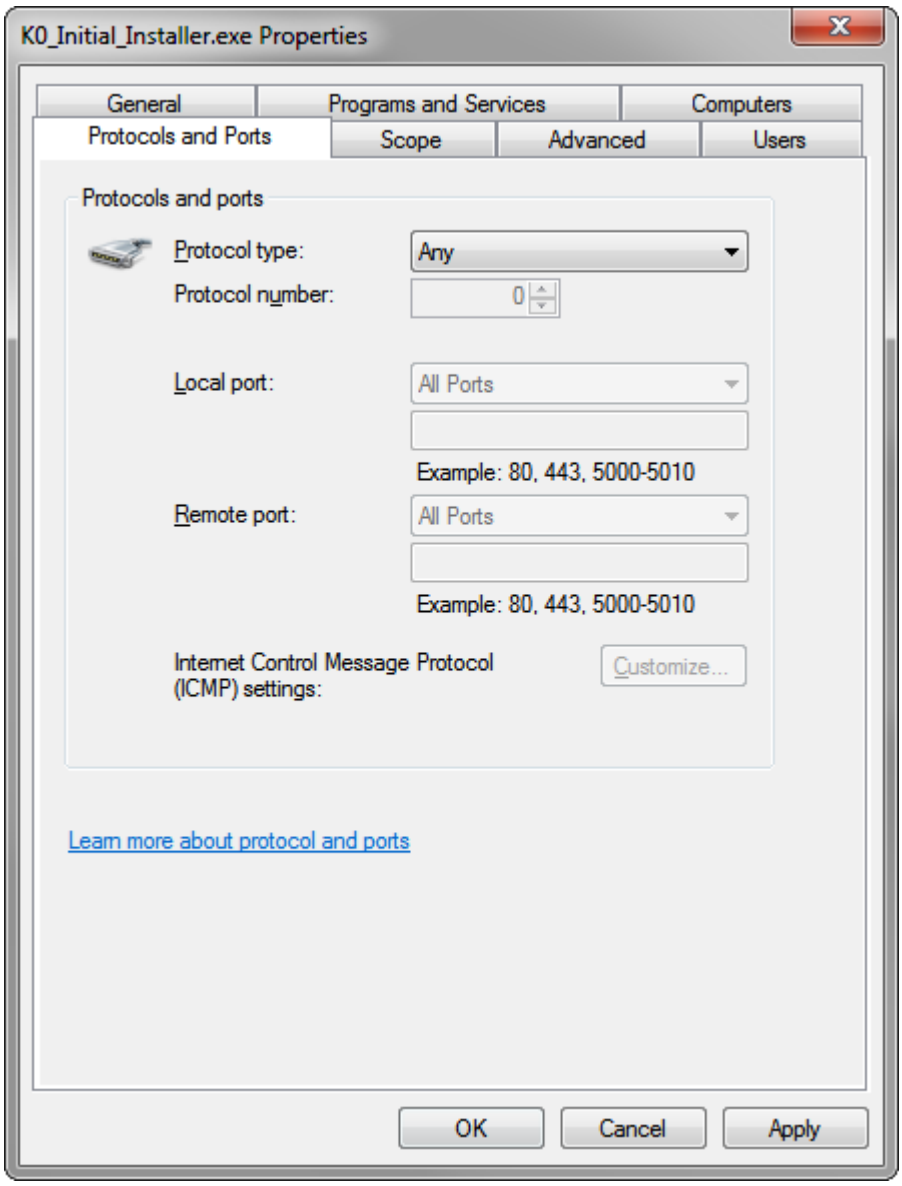
Next click Advanced settings on the Windows Firewall Settings Menu shown above.

Click Inbound Rules. Right click on K0_Initial_Installer.exe -> Properties -> Make sure Enabled & Allowed are checked.





Then go to the Protocols and Ports Tab -> Protocol Type -> Any -> Apply -> OK.



Hit Apply. Then OK. Now close all of the Windows and you should be able to use the Initial Installer to upgrade your RTU to the latest Firmware.