

Windows 7 Firewall Configuration

DATE: 13 DECEMBER 2011

SOFTWARE VERSION AND BUILD: VERSION 2.7.26 b228 AND HIGHER

DOCUMENT PERTAINS TO: CONFIGURING THE WINDOWS FIREWALL
ON A WINDOWS 7 COMPUTER.

REVISION: REV A



DISCLAIMER

Continental Instruments LLC makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Continental Instruments LLC reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Continental Instruments LLC to notify any person of such revision or changes. If possible, always refer to the Continental Access website (www.cicaccess.com); click **Support**) for the latest documentation, as the released CD may not contain the latest documentation.

Copyright © 2011 by Continental Instruments LLC. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, or stored in a retrieval system, without the prior written permission of Continental Instruments LLC, 355 Bayview Avenue, Amityville, NY 11701. Telephone: 631-842-9400 • FAX: 631-842-9135 • GSA# GS-07F-0039H.

ProxCard® and ProxKey® are trademarks of the HID® Corporation. Microsoft® and Windows® are trademarks of their the Microsoft Corporation. Trilogy® is a registered trademark of Alarm Lock. All other trademarks, service marks, and product or service names described in this manual are for identification purposes only and may be trademarks or registered trademarks of their respective owners.

The absence of a name or logo in this document does not constitute a waiver of any and all intellectual property rights that NAPCO Security Technologies, Inc. or Continental Instruments LLC has established in any of its product, feature, or service names or logos.

This document contains proprietary information of NAPCO Security Technologies. Unauthorized reproduction of any portion of this manual without the written authorization of NAPCO Security Technologies is prohibited. The information in this manual is for informational purposes only. It is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. NAPCO Security Technologies assumes no responsibility for incorrect information this manual may contain.

A NAPCO SECURITY TECHNOLOGIES COMPANY

Publicly traded on NASDAQ Symbol: NSSC

Visit our websites at

<http://www.cicaccess.com/>

<http://www.napcosecurity.com/>

<http://www.alarmlock.com/>

Table of Contents

Overview	4
CardAccess 3000 TCP/IP Ports	4
Firewall settings in Services/Control Panel	5
Windows Firewall	6
Windows Firewall with Advanced Security	7
Domain Profile settings	8
Private Profile settings	9
Public Profile settings	10

Overview

OVERVIEW

This document provides a quick reference for configuring the Windows 7 firewall for use with the CardAccess 3000 software. This document is intended to be used on a CardAccess 3000 host computer. The settings provided in this document open all ports, allowing the CardAccess 3000 software to function. If the IT department requires only specific ports to be opened, it is their responsibility to create all the exceptions and rules. Within this document is a list of all the ports used by CardAccess 3000 software and the Lantronix network interface unit.

CARDACCESS 3000 TCP/IP PORTS

The following ports are used for the CardAccess 3000 software:

- **ECHO Port 7:** This port is used by ICMP for Ping Request . This port is also used to keep existing Lines of communication open.
- **80:** This Port is used by the Graphic User interface for the Lantronix device (GUI)
- **1433:** This port is used by Microsoft SQL Server and MSDE. TCP/IP
- **1434:** This port is used by Microsoft SQL and MSDE. UDP. TCP/IP
- **3001:** This port is used by CardAccess 3000 to communicate with the panels through Lantronix devices. The Redirector software is not used in this case.
- **9000:** This port is used by CICDataServer for broadcasting information to the workstations.
- **9999:** This Port is used by the Lantronix Device for the use of the Telnet feature.
- **14001:** This port is used by CardAccess 3000 to communicate with the panels through Lantronix devices using the Redirector software. Only required for use with Windows NT 4.0 SP6
- **10001:** This port is used by the Trilogy Networkx Wireless lock (Gateway listens on this port).
- **5001:** This port is used by the Trilogy Networkx Wireless lock (CardAccess 3000 host listens on this port).

Firewall Settings In Services/Control Panel

WINDOWS FIREWALL IN SERVICES

1) Right click on **COMPUTER**. Click **MANAGE** and then select **Services and Applications**. Under **Services**, verify the Windows Firewall is **Started** and set to **Automatic** as per figure 1.

Windows Event Log	This servic...	Started	Automatic	Local Service
Windows Firewall	Windows Fi...	Started	Automatic	Local Service
Windows Font Cac...	Optimizes ...	Started	Automatic (D...	Local Service
Windows Image Ac...	Provides im...		Manual	Local Service
Windows Installer	Adds, modi...		Manual	Local System

Figure 1.

WINDOWS FIREWALL IN CONTROL PANEL

2) In Control Panel, click Windows Firewall (Refer to figure 2).



Figure 2.

Windows Firewall

WINDOWS FIREWALL

3) Click Advanced Settings (Refer to figure 3).

Windows Firewall

Control Panel > All Control Panel Items > Windows Firewall

Control Panel Home

- Allow a program or feature through Windows Firewall
- Change notification settings
- Turn Windows Firewall on or off
- Restore defaults
- Advanced settings**
- Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?
What are network locations?

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

[Use recommended settings](#)

Home or work (private) networks

Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Allow all connections that do not have an exception to block the connection
Active home or work (private) networks:	Network 3
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks

Not Connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Allow all connections that do not have an exception to block the connection
Active public networks:	None
Notification state:	Notify me when Windows Firewall blocks a new program

See also

- Action Center
- Network and Sharing Center

Figure 3.

Windows Firewall with Advanced Security

WINDOWS FIREWALL WITH ADVANCED SECURITY

4) Right Click on **Windows Firewall with Advanced Security**. Select **Properties** (Refer to figure 4).

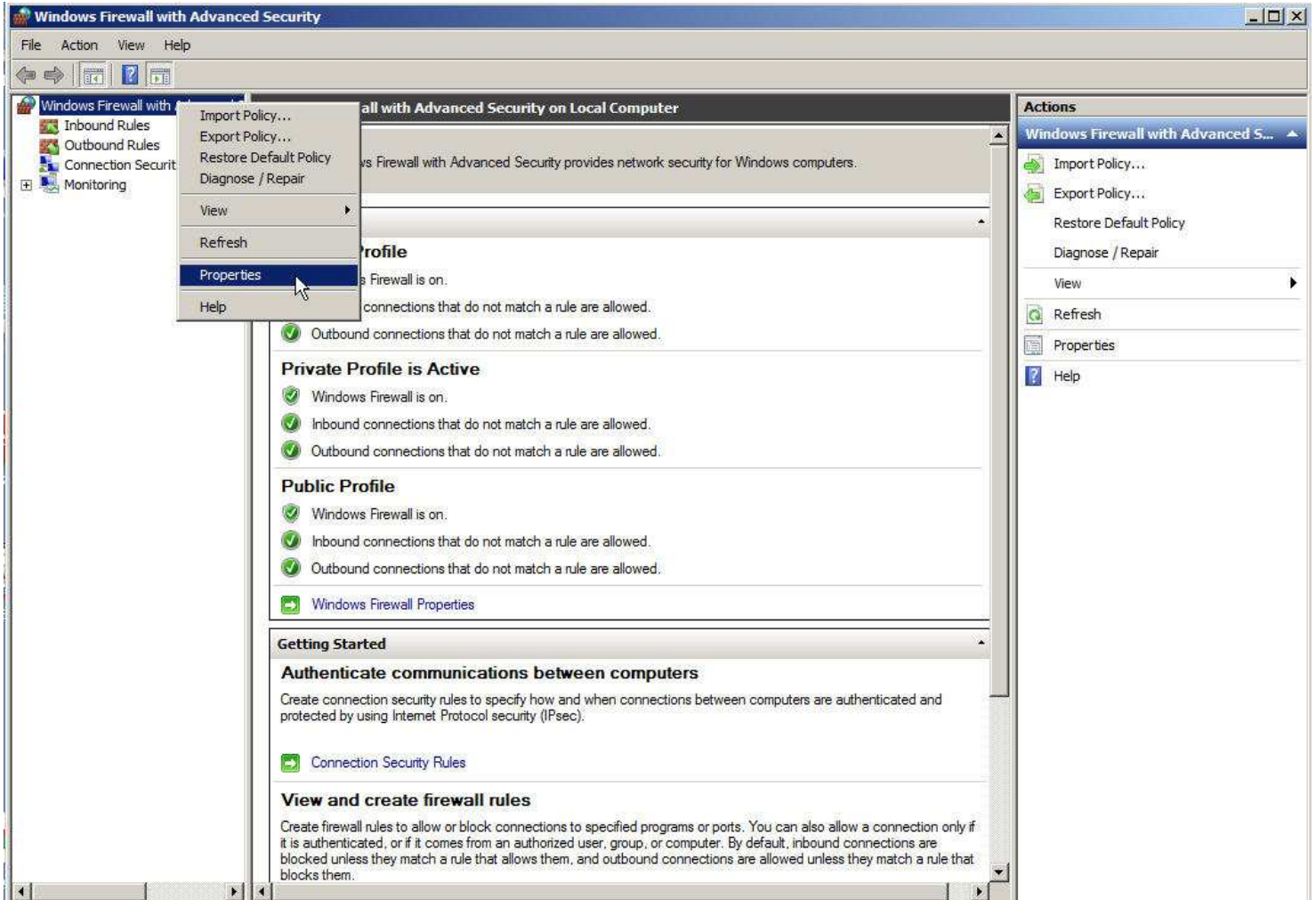


Figure 4.

Domain Profile

DOMAIN PROFILE SETTINGS

5) Click the **Domain Profile** Tab. Configure as per figure 5).

Firewall State : On (recommended)

Inbound connections: Allow

Outbound connections: Allow (default)

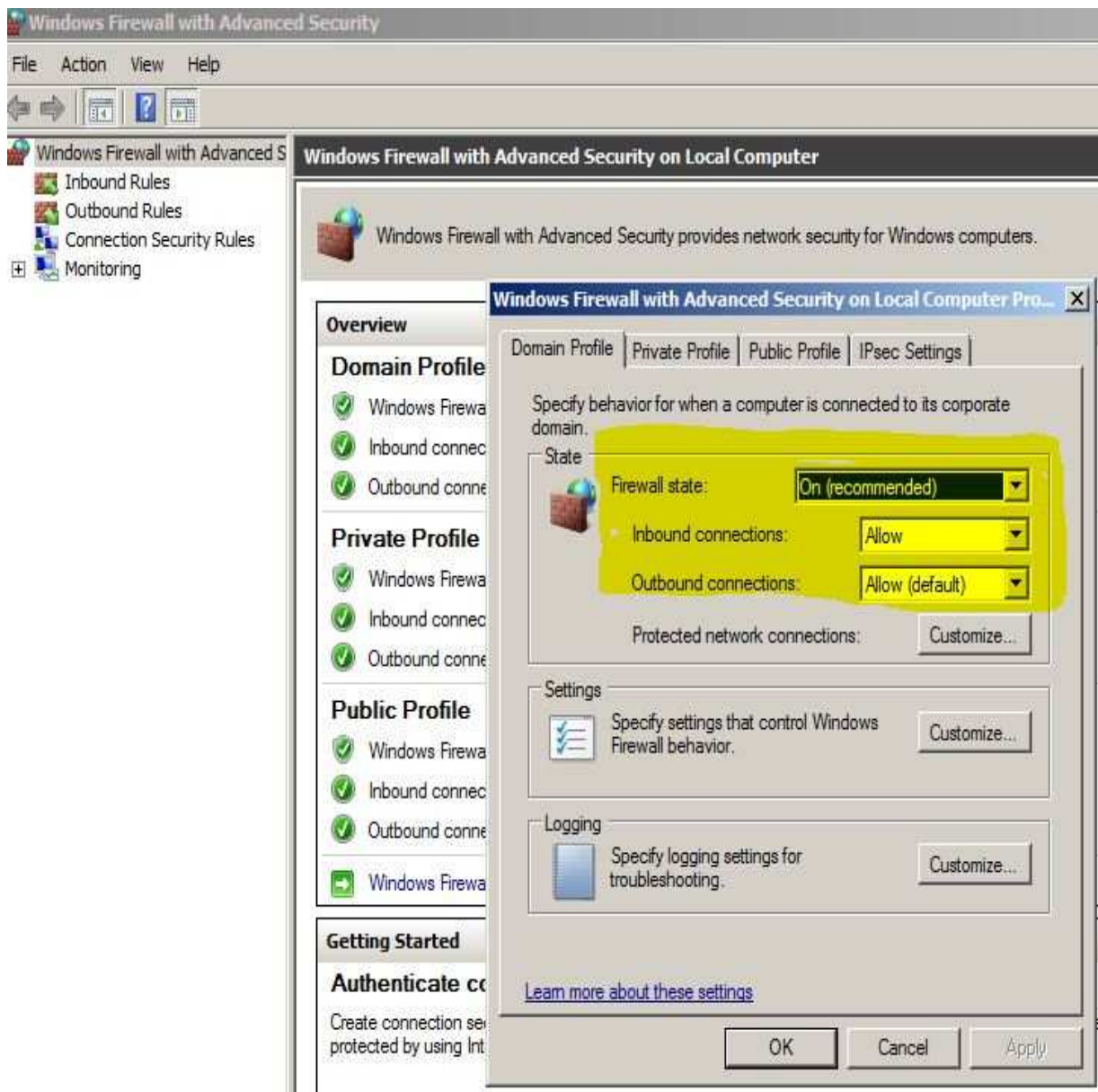


Figure 5.

Private Profile

PRIVATE PROFILE SETTINGS

6) Click the **Private Profile** Tab. Configure are per figure 6.

Firewall State : On (recommended)

Inbound connections: Allow

Outbound connections: Allow (default)

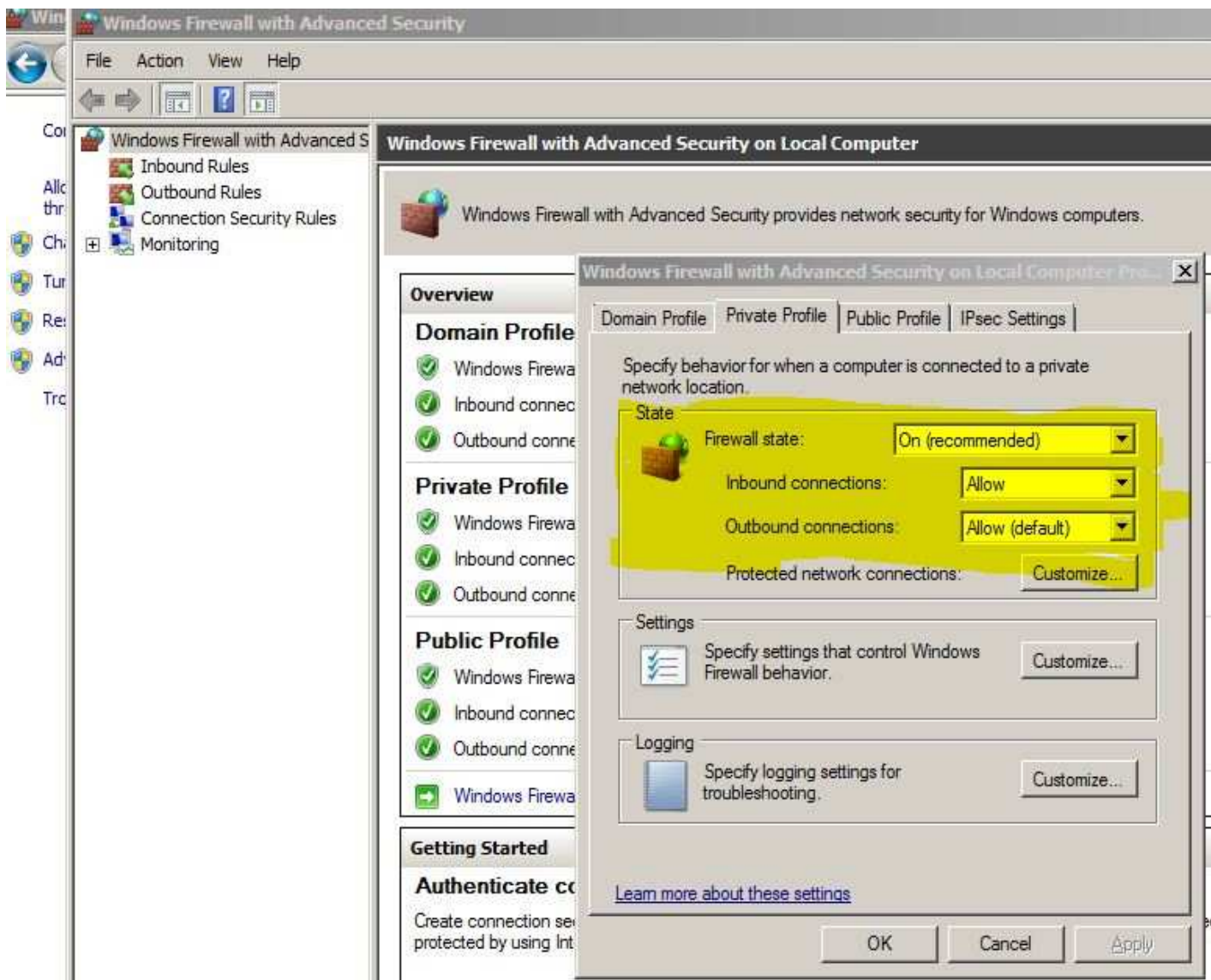


Figure 6.

Public Profile

PUBLIC PROFILE SETTINGS

7) Click the **Public Profile** Tab. Configure are per figure 7.

Firewall State : On (recommended)

Inbound connections: Allow

Outbound connections: Allow (default)

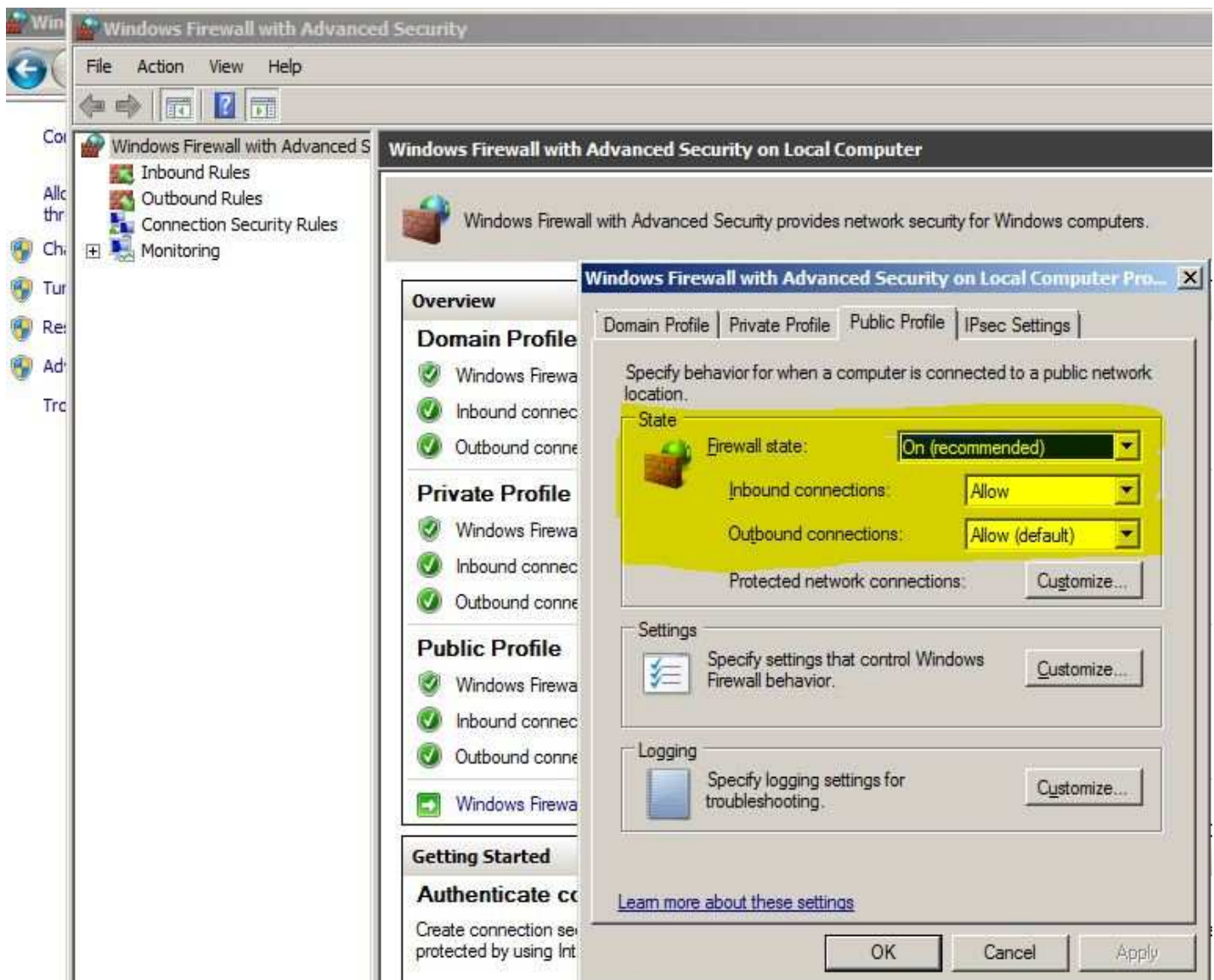


Figure 7.