Securing Windows 7

Lesson 10

Objectives

- Understand authentication and authorization
- Configure password policies
- Secure Windows 7 using the Action Center
- Configure Windows Firewall
- Protect sensitive data
- Configure parental controls

Authenticating and Authorizing Users

Two of the most important functions of Windows 7:

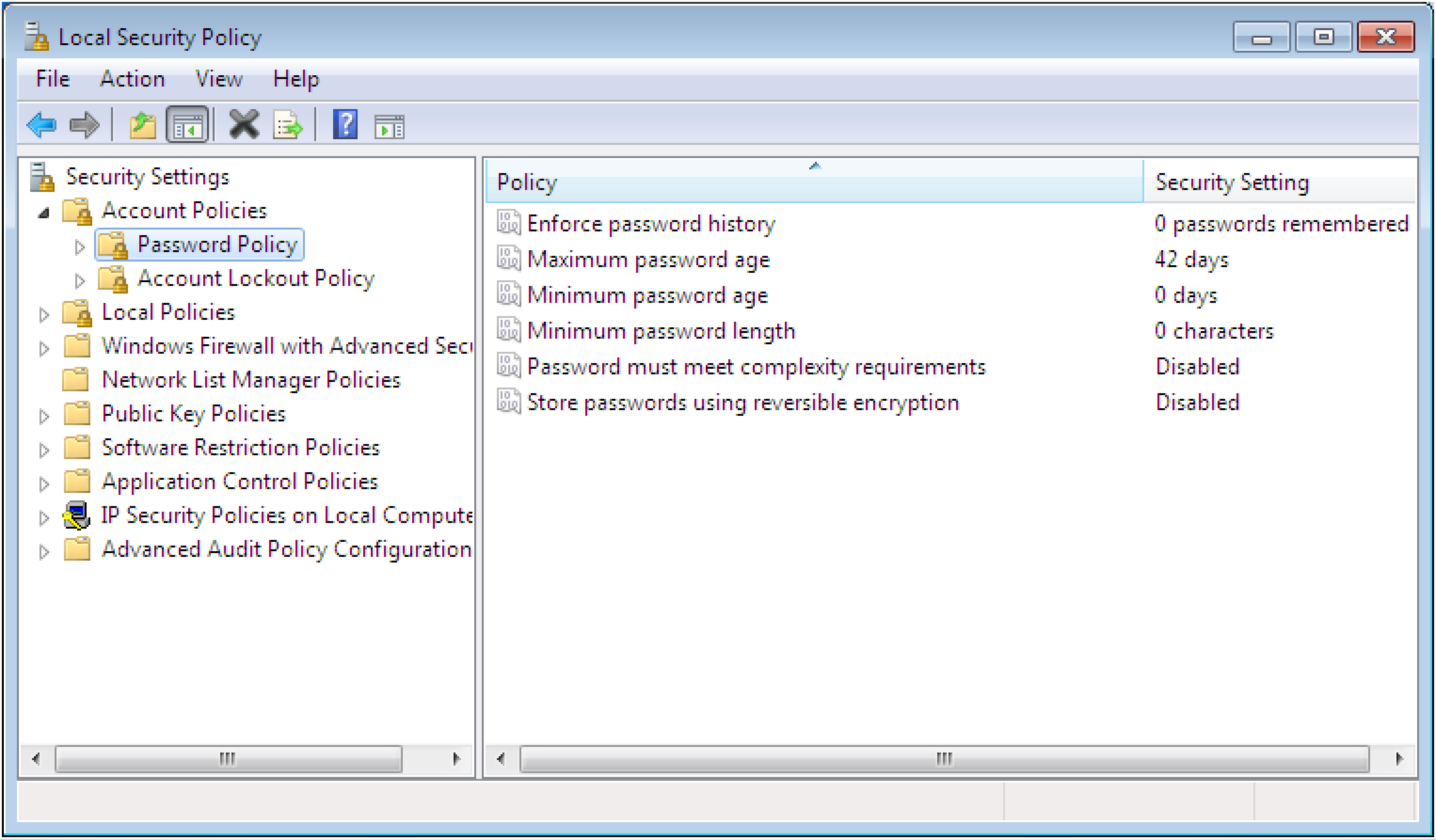
Authentication: Confirms the identity of a user

Authorization: Specifies which resources the user is permitted to access

Configuring Password Policies

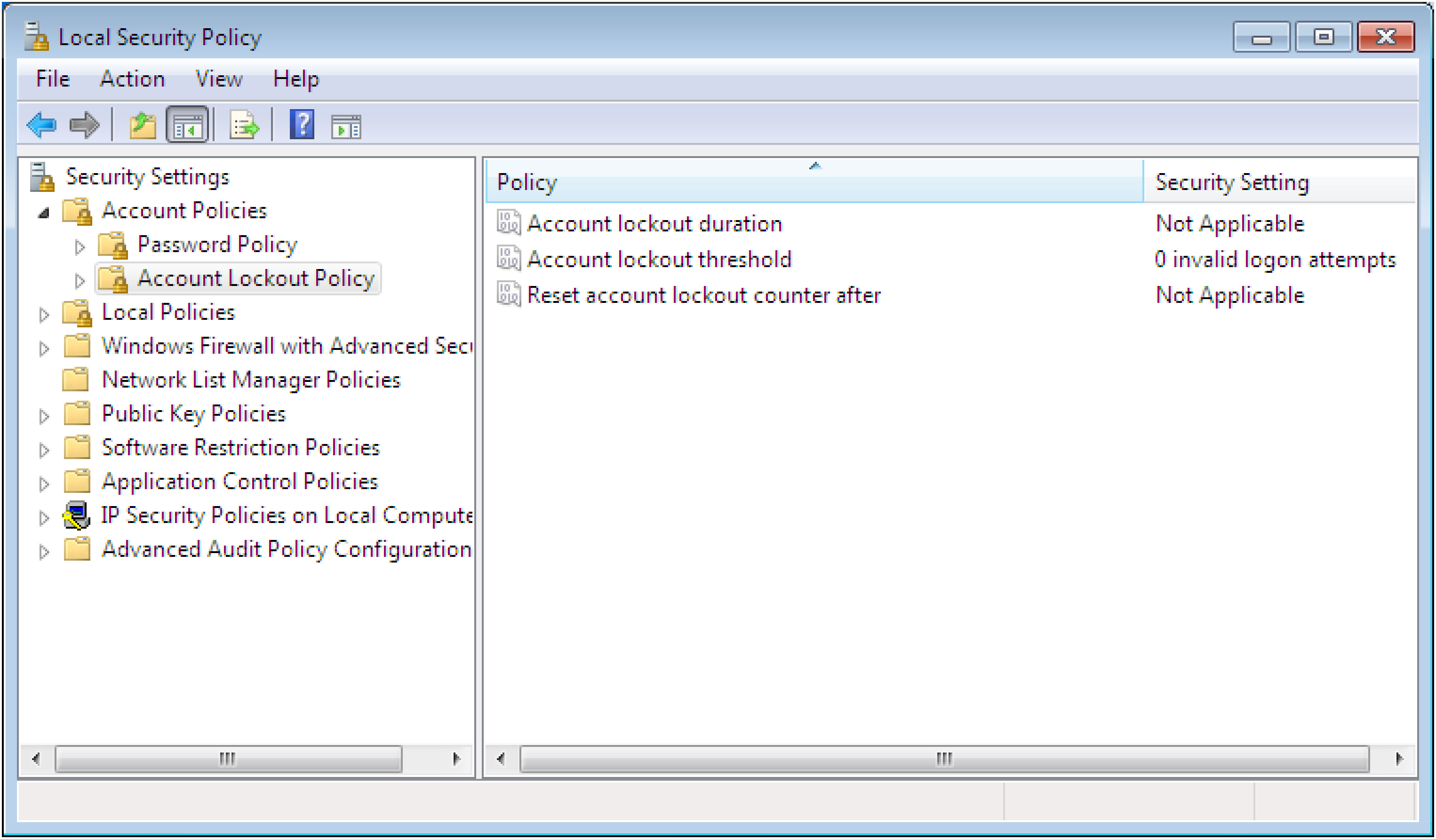
- Used to enforce good password security practices
- Local Security Policy on individual computers, or Group Policy on an AD DS

Password Policy


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

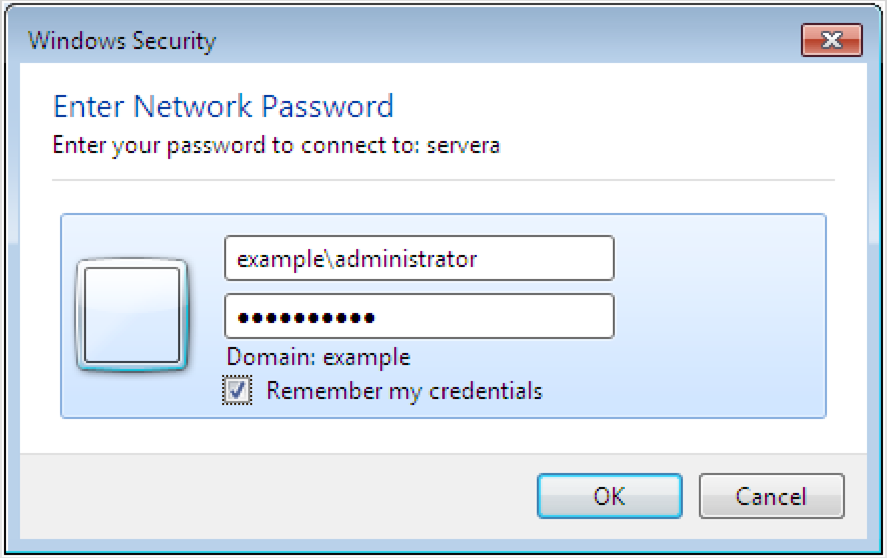
Account Lockout Policies


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

Using Credential Manager

- Stores usernames and passwords for servers and Web sites in Windows Vault
- Remember my credentials checkbox adds credentials to the Windows Vault



Windows Security

Enter Network Password

Enter your password to connect to: servera

example\administrator

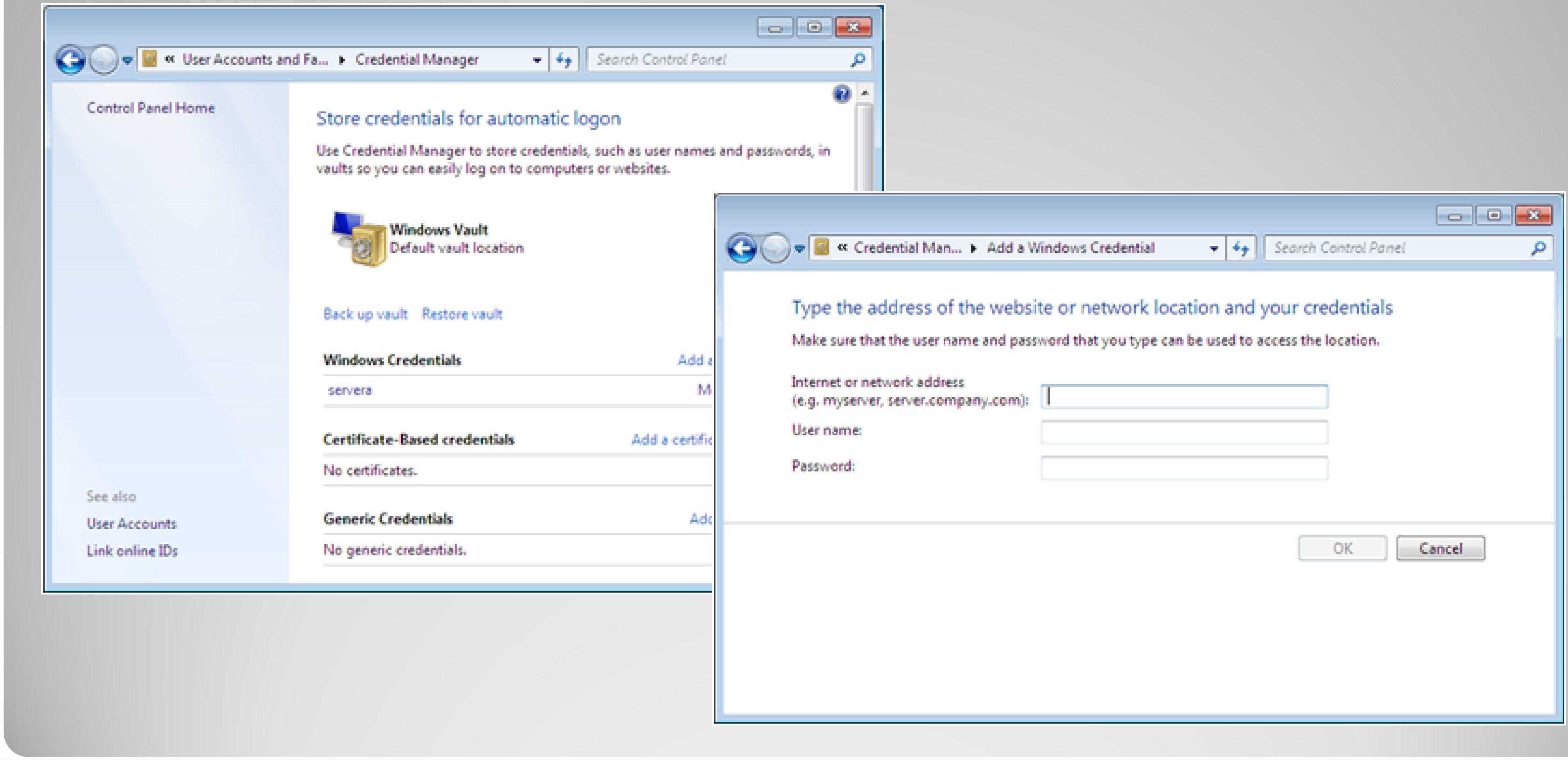
●●●●●●●●●●●

Domain: example

☑ Remember my credentials

Using Credential Manager

- Credentials can be added directly



Store credentials for automatic logon

Use Credential Manager to store credentials, such as user names and passwords, in vaults so you can easily log on to computers or websites.

Windows Vault
Default vault location

Windows Credentials — Add a
servera — M

Certificate-Based credentials — Add a certific
No certificates.

Generic Credentials — Add
No generic credentials.

Type the address of the website or network location and your credentials

Make sure that the user name and password that you type can be used to access the location.

Internet or network address
(e.g. myserver, server.company.com):

User name:

Password:

Smart Cards

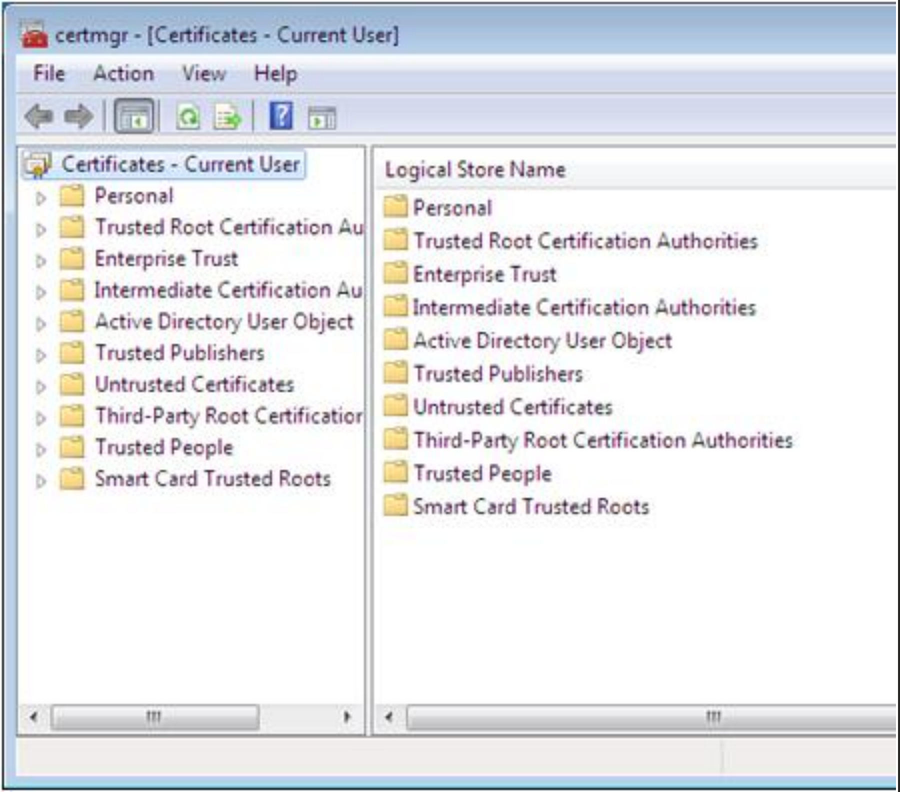
- High security alternative to passwords
- Requires the use of a credit card-like device
- Support for Smart Cards built into Windows 7
- Group Policy controls how authentication with Smart Cards is enforced

Managing Certificates

- Used for a variety of authentication tasks, internally, on the local network, and on the Internet.
- Windows 7 maintains a certificate store for each user – Automated
- Users can manage their certificate stores directly using Certificates snap-in

Certificates Snap-In

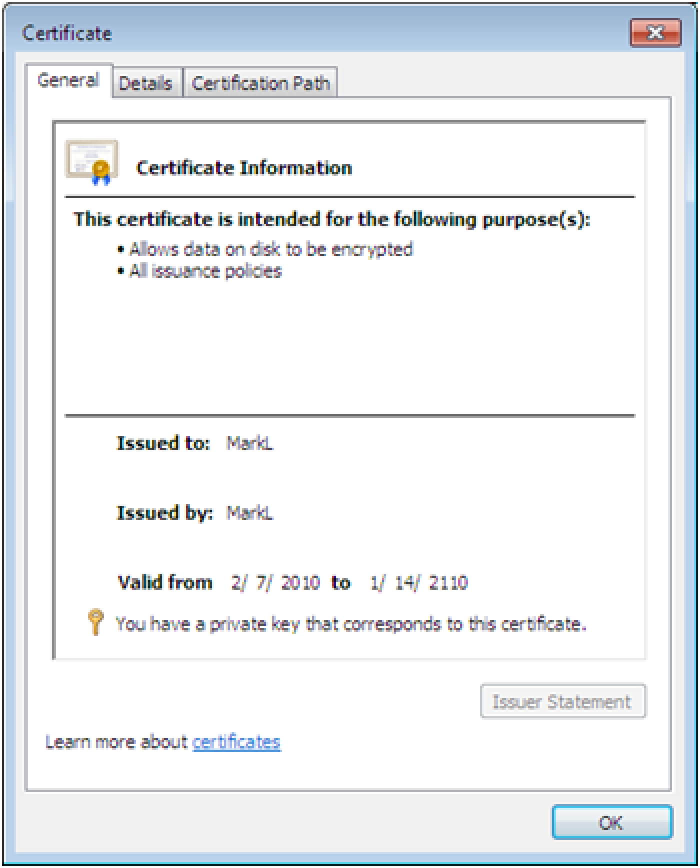
- Certmgr.msc



certmgr - [Certificates - Current User]

Certificates - Current User
- Personal
- Trusted Root Certification Au
- Enterprise Trust
- Intermediate Certification Au
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certificatior
- Trusted People
- Smart Card Trusted Roots

Logical Store Name
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Smart Card Trusted Roots



Certificate

Certificate Information

This certificate is intended for the following purpose(s):
- Allows data on disk to be encrypted
- All issuance policies

Issued to: MarkL

Issued by: MarkL

Valid from 2/ 7/ 2010 **to** 1/ 14/ 2110

You have a private key that corresponds to this certificate.

Learn more about certificates

Using Biometrics

- Scans a physical characteristic of a user to confirm identity
- *Windows Biometric Framework* provides core biometric functionality and a Biometric Device control panel

Elevating Privileges

- Use *Run As Administrator* context menu option
- Use command line *runas.exe* command:

```
runas /user:example\administrator
“notepad.exe\script.vbs”
```

Troubleshooting Authentication Issues

- Password loss is the most common problem.
- There is no way for an administrator to read a password.
- Passwords must be reset.
- Users can change their own password if they know their old password.
- Administrator can reset password without supplying old password.
- Password reset Disk is better option.

Authorizing Users

- Authorization grants the user access to certain resources:
  - Using permissions
  - Configuring user rights

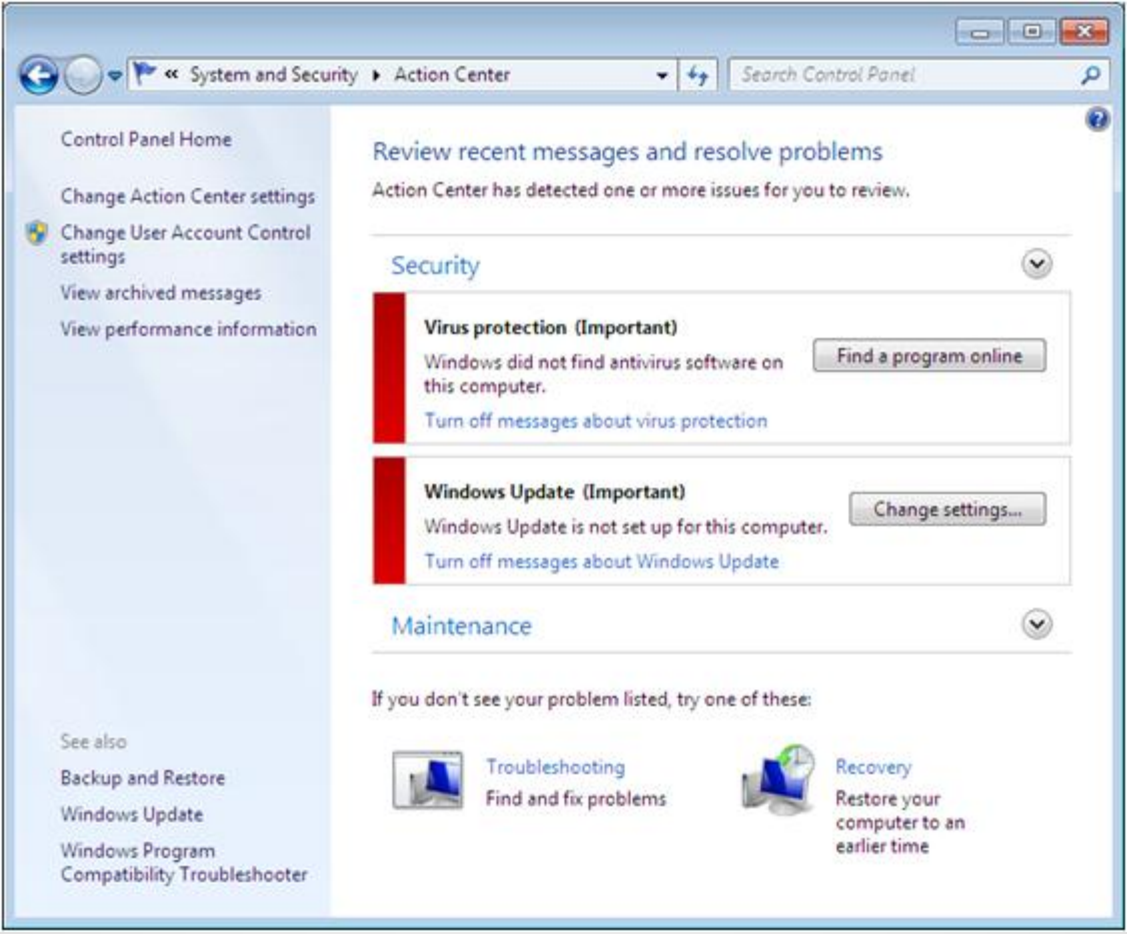
Defending Against Malware

- Malware: Malicious software created specifically for the purpose of infiltrating or damaging a computer system without the user's knowledge or consent
- Viruses
- Trojan horses
- Worms
- Spyware
- Adware

Security in Windows 7

- Lesson 7, “Working with Applications,” you learn about the security features included in Internet Explorer 8.
- Lesson 9, “Working with Workgroups and Domains,” you learn how User Account Control helps to prevent malware from obtaining administrative privileges.
- Lesson 12, “Working with Mobile Computers,” you learn about the security features specifically designed for use on mobile and wireless computers.

Introducing Windows 7 Action Center



« System and Security ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
View archived messages
View performance information
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

Action Center has detected one or more issues for you to review.

Security

Virus protection (Important)

Windows did not find antivirus software on this computer.

Turn off messages about virus protection

Windows Update (Important)

Windows Update is not set up for this computer.

Turn off messages about Windows Update

Maintenance

If you don't see your problem listed, try one of these:

Troubleshooting
Find and fix problems

Recovery
Restore your computer to an earlier time

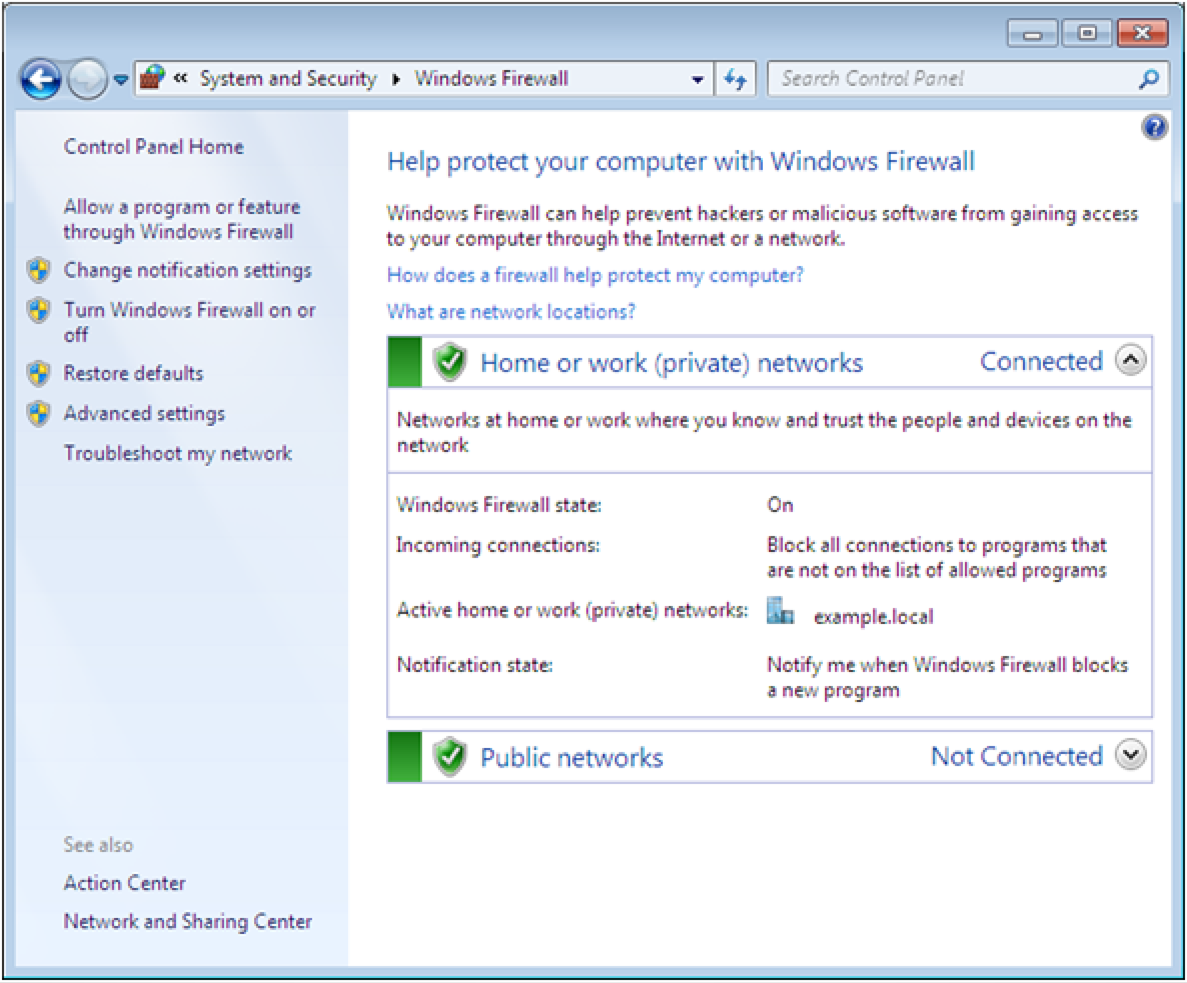
Introducing Windows Firewall

- A *firewall* is a software program that protects a computer by allowing certain types of network traffic in and out of the system while blocking others.

Understanding Firewalls

- Base their filtering on TCP/IP characteristics:
  - IP address - Specific computers
  - Protocol numbers - Transport layer protocol
  - Port number - Application running on computer
- **Rules** are used to filter traffic two ways:
  - Admit all traffic, except that which applies to the rules
  - Block all traffic, except that which applies to the rules

The Windows Firewall Window


« System and Security ▸ Windows Firewall
Search Control Panel
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
See also
Action Center
Network and Sharing Center

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?

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

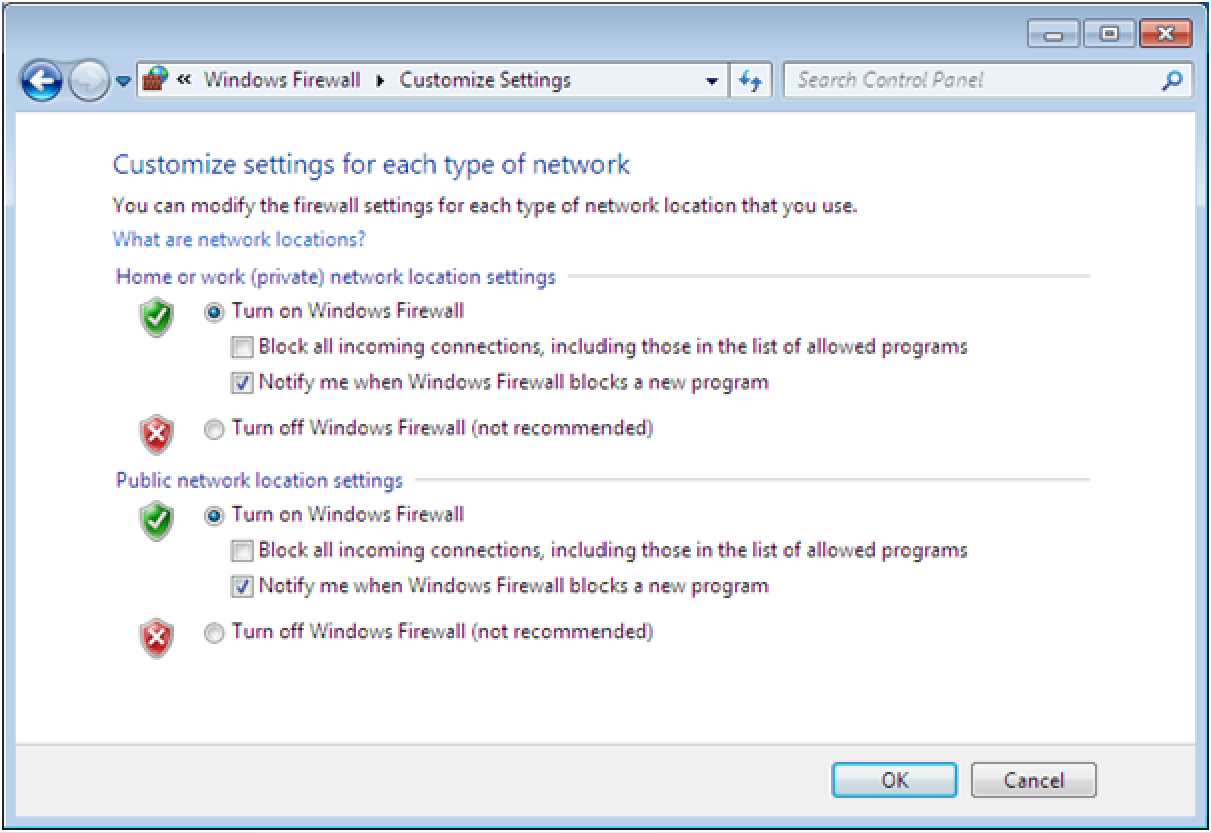
Incoming connections: Block all connections to programs that are not on the list of allowed programs

Active home or work (private) networks: example.local

Notification state: Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

Using the Windows Firewall Control Panel



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

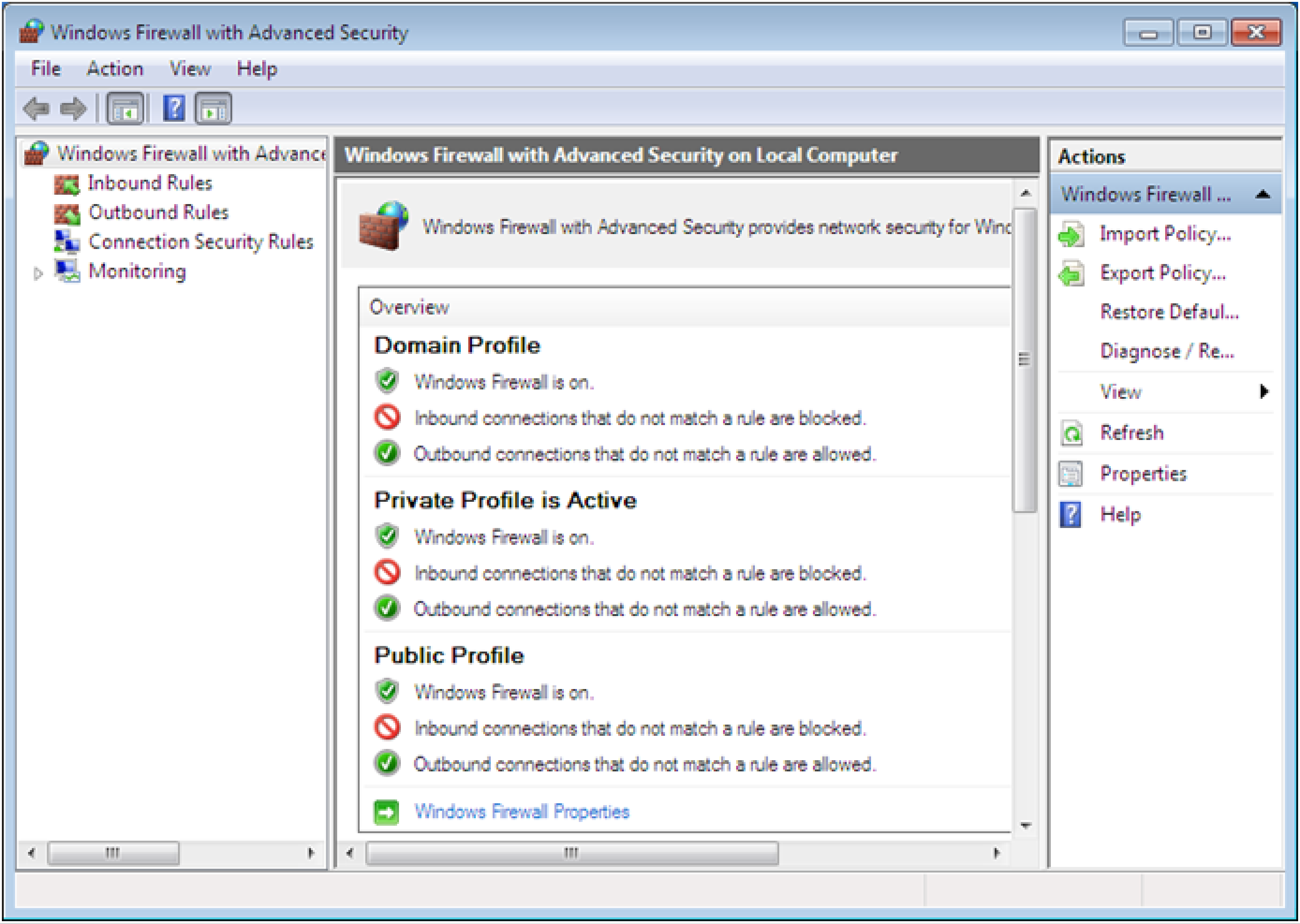
● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Using the Windows Firewall with Advanced Security Console



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Winc

Overview

Domain Profile

✓ Windows Firewall is on.

⃠ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Private Profile is Active

✓ Windows Firewall is on.

⃠ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Public Profile

✓ Windows Firewall is on.

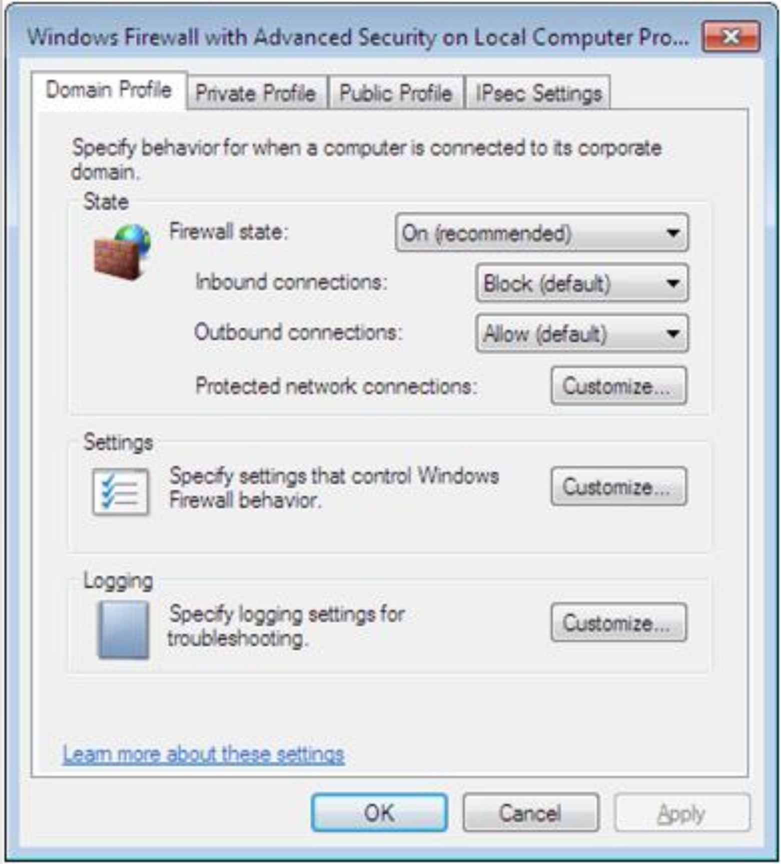
⃠ Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Using the Windows Firewall with Advanced Security Console

- Default profile settings can be modified
- Inbound and outbound rules can be created



Windows Firewall with Advanced Security on Local Computer Pro...

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

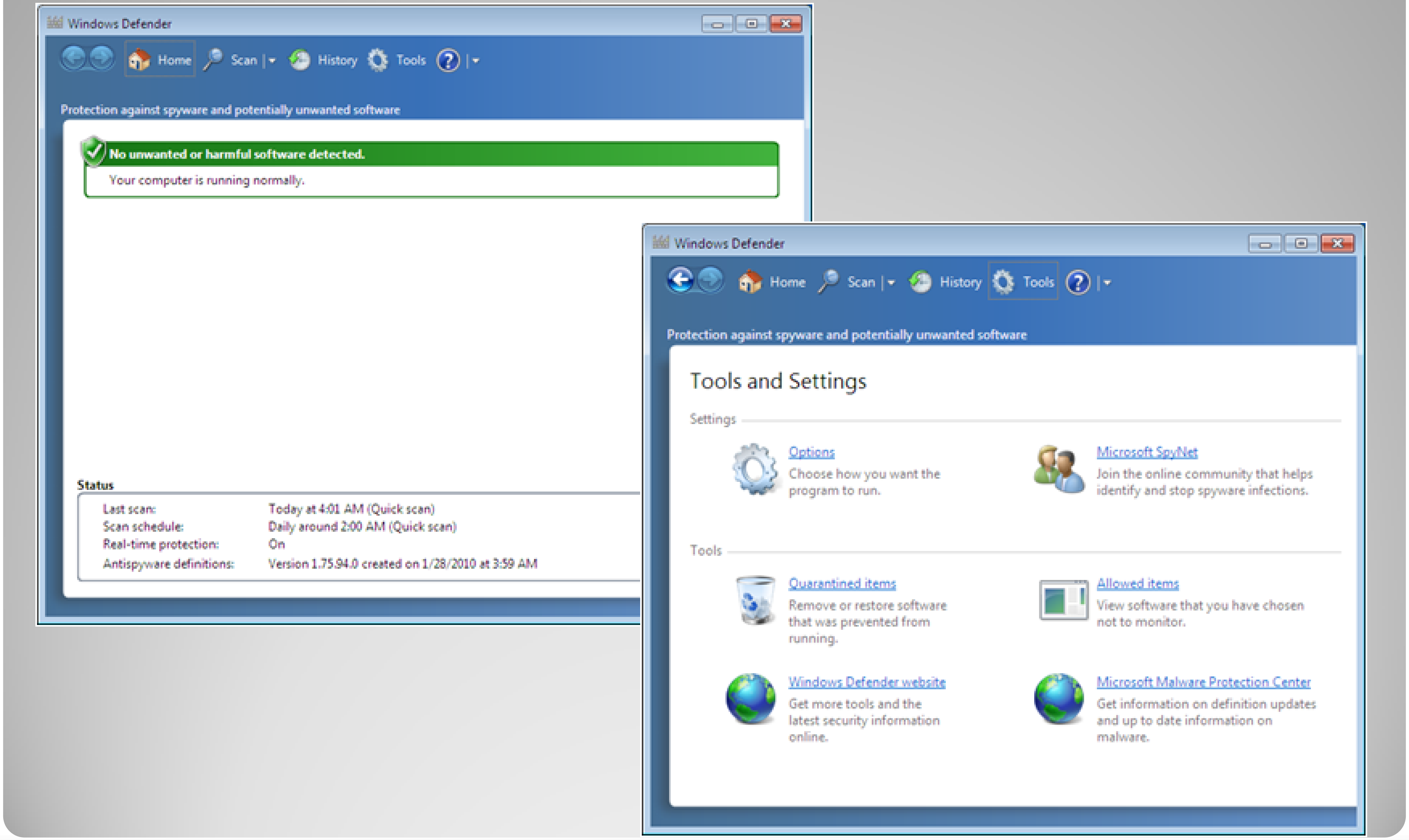
Specify settings that control Windows Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

Learn more about these settings

Introducing Windows Defender



Protection against spyware and potentially unwanted software

No unwanted or harmful software detected.

Your computer is running normally.

Status

Last scan:	Today at 4:01 AM (Quick scan)
Scan schedule:	Daily around 2:00 AM (Quick scan)
Real-time protection:	On
Antispyware definitions:	Version 1.75.94.0 created on 1/28/2010 at 3:59 AM

Protection against spyware and potentially unwanted software

Tools and Settings

Settings

Options
Choose how you want the program to run.

Microsoft SpyNet
Join the online community that helps identify and stop spyware infections.

Tools

Quarantined items
Remove or restore software that was prevented from running.

Allowed items
View software that you have chosen not to monitor.

Windows Defender website
Get more tools and the latest security information online.

Microsoft Malware Protection Center
Get information on definition updates and up to date information on malware.

Malicious Software Removal Tool

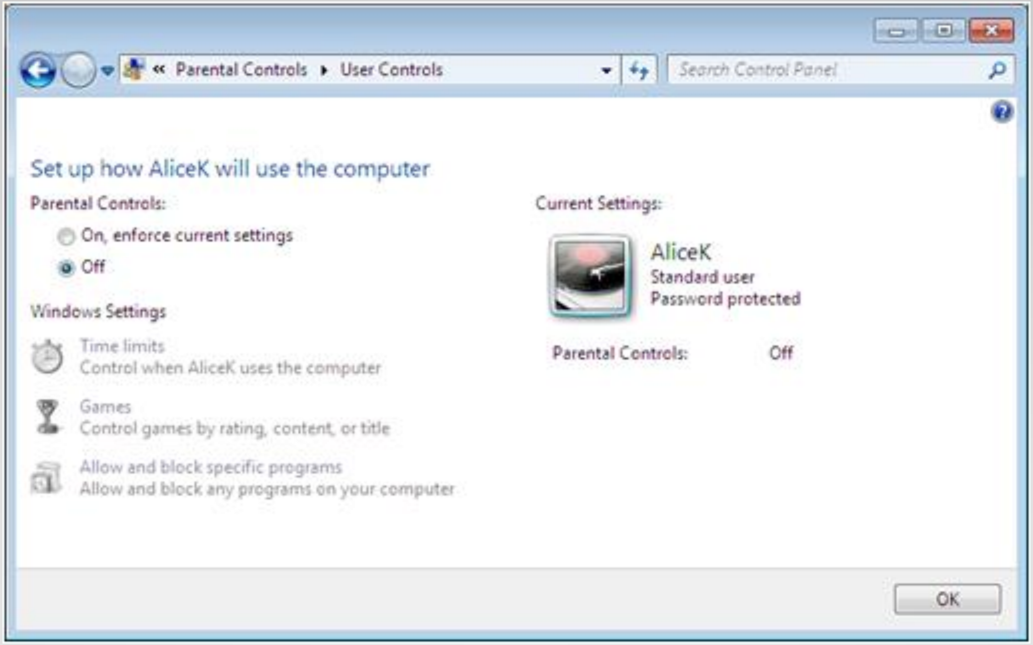
- A single user virus scanner supplied with monthly updates
- Removes any potentially damaging software it finds
- There are no controls and is not permanently installed
- Should install a full-featured antivirus program on Windows 7

Using the Encrypting File System (EFS)

- EFS is a feature of NTFS that encodes the files on a computer.
- The system is keyed to a specific user account.
- Uses *public* and *private* keys (PKI).
- The user who creates the file is the only person who can read it.

Configuring Parental Controls

Parental controls enables parents to limit their children’s access to specific Internet sites, games, and applications.



Set up how AliceK will use the computer

Parental Controls:

○ On, enforce current settings

● Off

Windows Settings

Time limits
Control when AliceK uses the computer

Games
Control games by rating, content, or title

Allow and block specific programs
Allow and block any programs on your computer

Current Settings:

AliceK
Standard user
Password protected

Parental Controls: Off

Setting Up Parental Controls

- Based on user accounts – Every family member must have their own account
- Impose restrictions on accounts
  - Filter Web sites users are allowed to access
  - Limit downloads from Internet sites
  - Enforce time limits for computer use
  - Restrict access to games by rating, content, or title
  - Allow or block specific applications

Skills Summary

- Password Policies enforce password security practices.
- Credential Manager is a tool that stores the user names and passwords people supply to servers and Web sites in a Windows Vault.
- Permissions and user rights are used to authorize users’ access to resources and tasks.
- Action Center is a centralized console that enables users and administrators to access, monitor, and configure the various Windows 7 security mechanisms.

Skills Summary (cont.)

- Windows Firewall is a software program that protects a computer by allowing certain types of network traffic in and out of the system while blocking others.
- Windows Defender helps to defend against spyware.
- The Malicious Software Removal Tool is a single user virus scanner.
- The Encrypting File System (EFS) is a feature of NTFS that encodes the files on a computer.