

Microsoft® Windows®

Paradigm
PUBLISHING

8

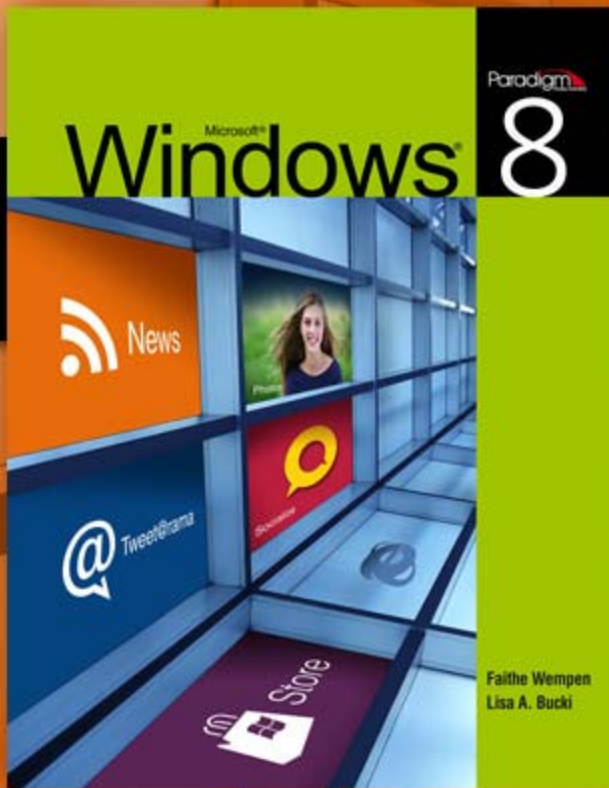


News

Photos



Faithe Wempen
Lisa A. Bucki

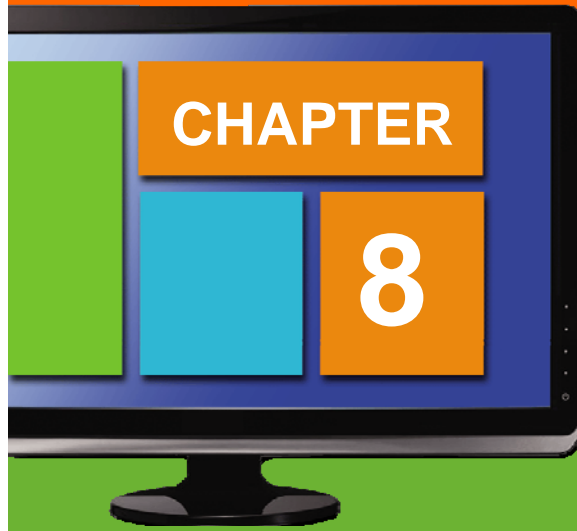


Chapter 8

Ensuring Your Safety and Privacy on the Internet

In This Chapter

- [Evaluating Your System's Overall Security Status](#)
- [Configuring Privacy Preferences](#)
- [Protecting the System with Windows Firewall](#)
- [Protecting Against Viruses and Other Malware with Windows Defender](#)

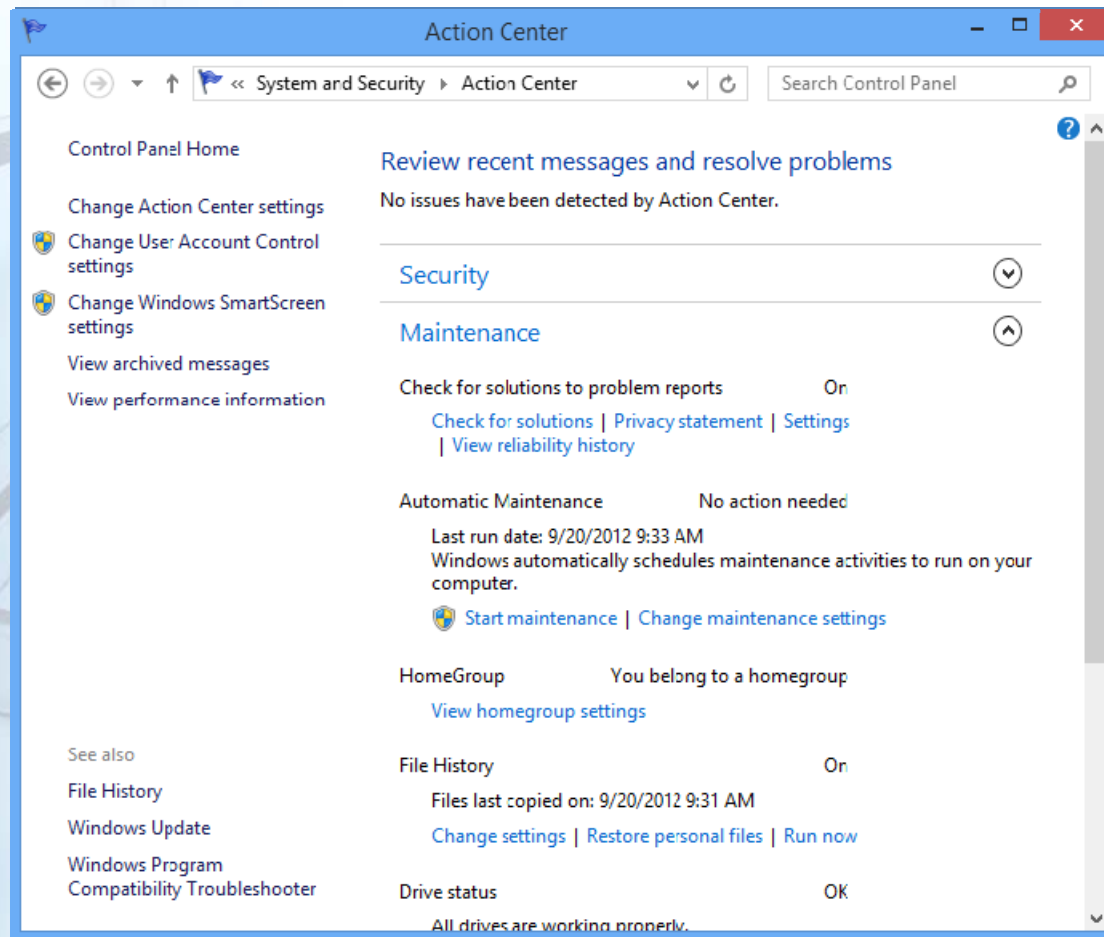


Evaluating Your System's Overall Security Status

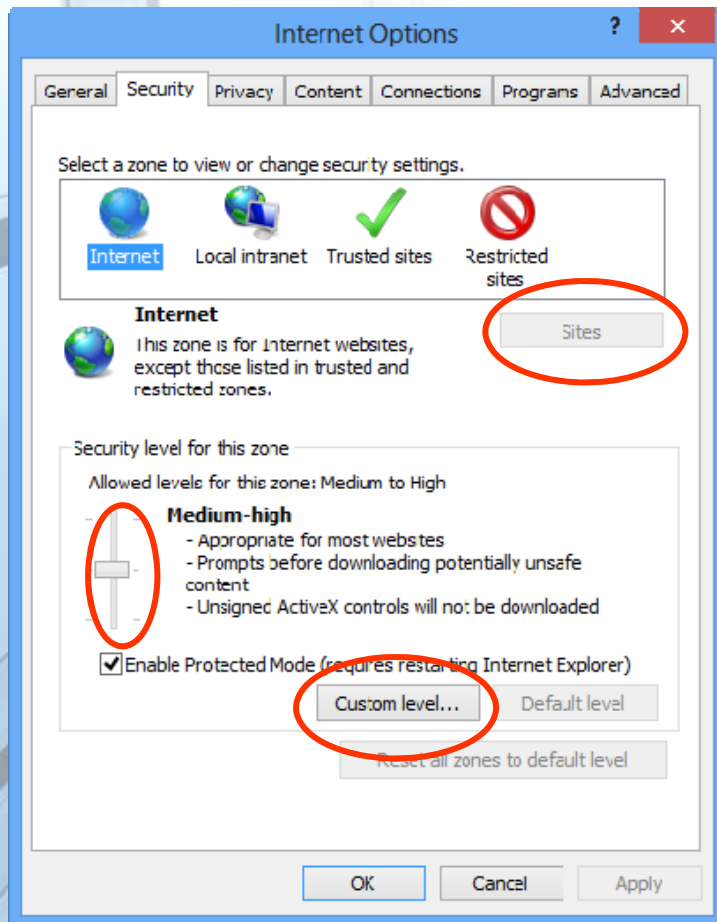
Evaluating Overall Security Status

- Use the Action Center to view status information about security utilities.
- In the Control Panel, under System and Security, click Review your computer's status to open the Action Center.
- Click a button in the Action Center to perform a quick fix on a security item.

Windows Action Center



Configuring Internet Security Zones



- Four security zones: Internet, Local intranet, Trusted sites, and Restricted sites.
- Choose Tools, Internet Options, and then click the Security tab to work with security settings.
- Click the zone icon and drag the slider to set the level, or set a custom level or add sites to a zone.

Configuring the Pop-Up Blocker

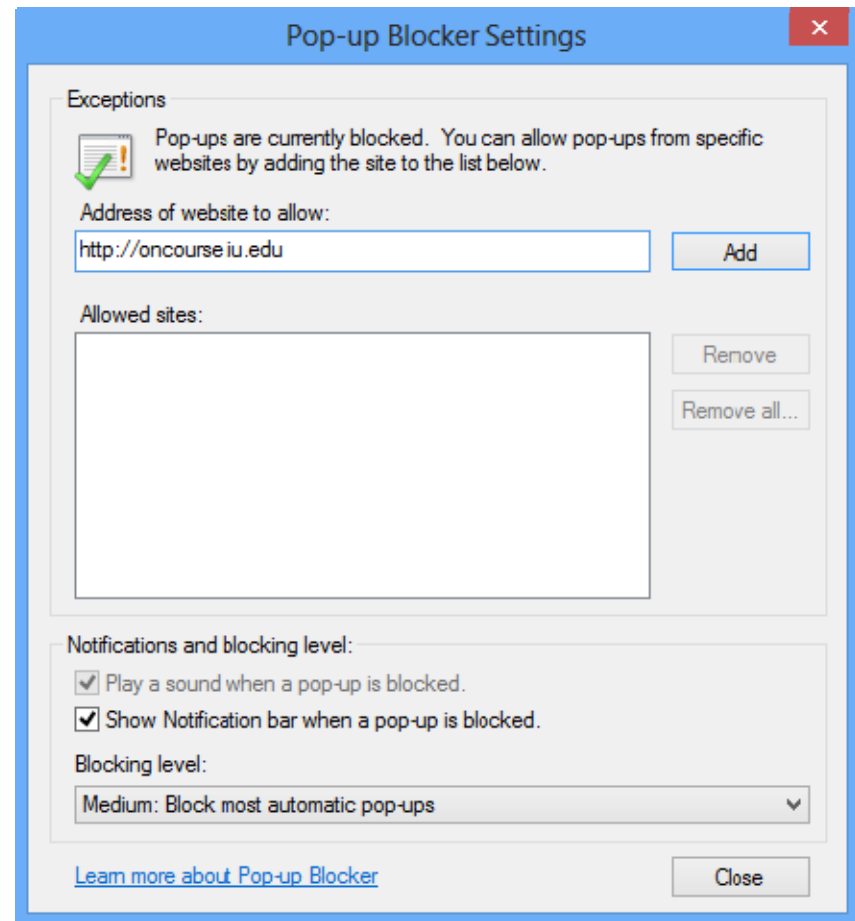
- A pop-up is an extra window with an ad or other information that appears when you go to a Web page.
- The pop-up blocker in IE enables you to block some or all pop-ups.
- The default filtering level is Medium, which blocks most pop-ups. You also can select High to block all pop-ups or Low to allow pop-ups from secure sites.

Configuring the Pop-Up Blocker

- To enable or disable Pop-up Blocker, choose Tools (menu), Pop-up Blocker, and click the Turn On Pop-up Blocker or Turn Off Pop-up Blocker command.
- Make sure you use the Tools menu on the menu bar. To display the menu bar, press Alt.

Configuring the Pop-Up Blocker

- To change the filtering level and add allowed sites, choose Tools (menu), Pop-up Blocker, and click Pop-up Blocker Settings.

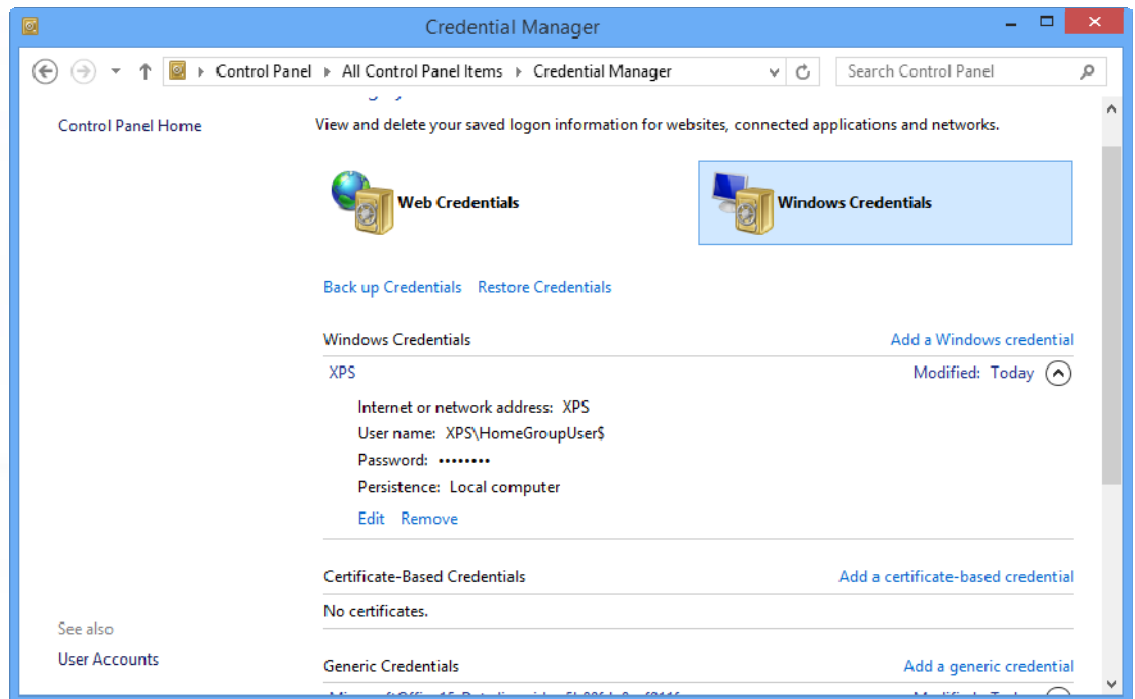


Managing Your Stored Credentials

- When you enter sign-in information at a website, IE asks if you want it to remember that info.
- When you revisit the same site, it fills in your user name and password automatically, saving you time.
- The Credential Manager in Windows 8 enables you to modify or delete those stored credentials.

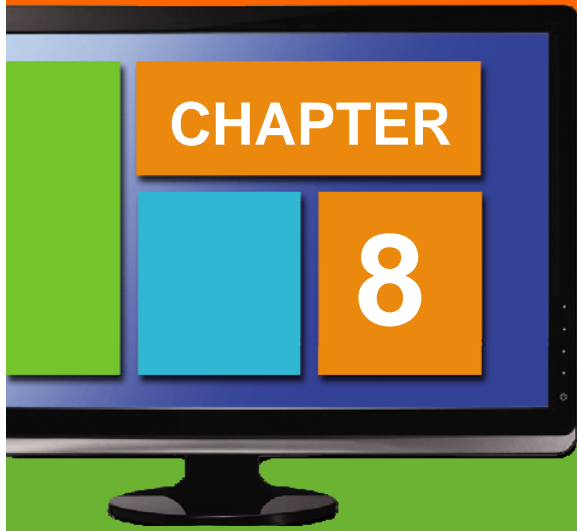
Deleting a Stored Web Credential

1. In Control Panel, click User Accounts and Family Safety.
2. Click Manage Windows Credentials.
3. Click Web Credentials.
4. Click the stored credential to delete.
5. Click Remove.
6. Click Yes.



Checkpoint

- Where do you view overall system security settings?
- What are Internet security zones?
- What is a pop-up and why are they undesirable?
- How do you turn the Pop-up Blocker on and off?
- What are credentials?



Configuring Privacy Preferences

Configuring Tracking Protection

- Some content on a website tracks your behavior across multiple sites.
- Tracking protection lets you choose what third-party websites can track your browsing activity.
- Tracking Protection Lists (TPL) are used to specify which third parties can receive your information and track you online.
- Get a TPL from www.iegallery.com.
- Manage TPLs by choosing Tools, Safety, Tracking Protection in IE.

Understanding Cookies

- Cookies are small, plain text files stored on the hard disk to track settings for certain Web sites.
- Session cookies are temporary. In contrast, persistent cookies are saved on the hard disk.
- First-party cookies are created by the Web site. In contrast, third-party cookies are created by ads to track marketing information.

Understanding Cookies

- Other local users can open the cookie files to gather your logon information.
- Deleting cookies prevents the problem, but eliminates the ability of IE to log on to certain sites automatically.

Blocking and Allowing Cookies

- To delete existing cookies in IE:
 - Choose Tools, Internet Options.
 - Click the General tab.
 - Click Delete under Browsing history.
 - Make sure Cookies is checked and click Delete.
 - Click OK.
- Also use the choices on the Privacy tab of the Internet Options dialog box to specify a cookie-handling policy.

Using InPrivate Browsing

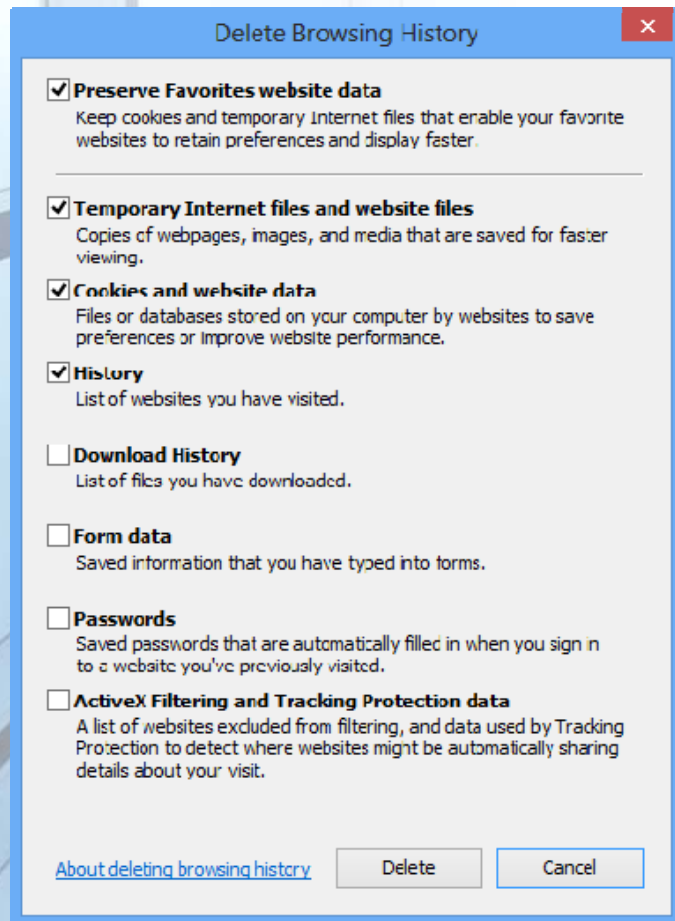
- The InPrivate Browsing mode enables you to browse a Web site without IE retaining any cookies, history, or temporary files.
- To activate InPrivate Browsing, choose Safety, InPrivate Browsing.
- Then use the Address bar to go to the desired page.



Clearing Browsing History and More

- IE stores temporary Internet files, cookies, history, form data, and passwords to make Web browsing easier.
- You can clear information to prevent unwanted access by other system users and to free disk space.
- You also can specify how many days of history the system tracks. The default is 20.
- Press Ctrl+Shift+H to display the history. You can then click a link to redisplay a page visited previously.

Clearing Personal Information

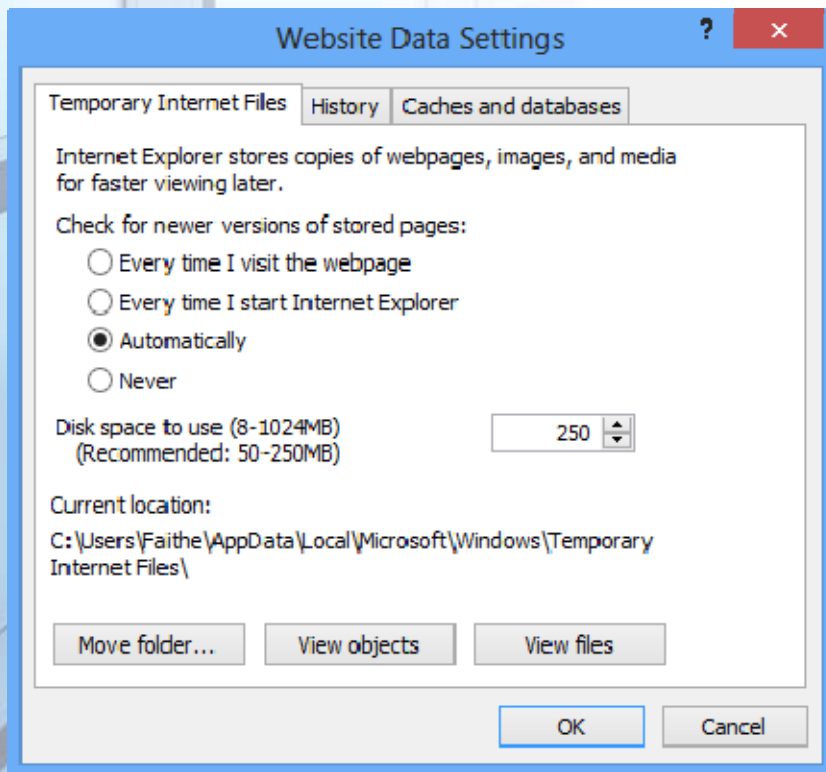


- Choose Safety, Delete Browsing History.
- Mark the check box for the type of content to delete and click Delete.

Specifying History to Store

- Choose Tools, Internet Options, and click the General tab.
- Click Settings in the Browsing History section.
- Enter the number of days for Days to keep pages in history and click OK twice.

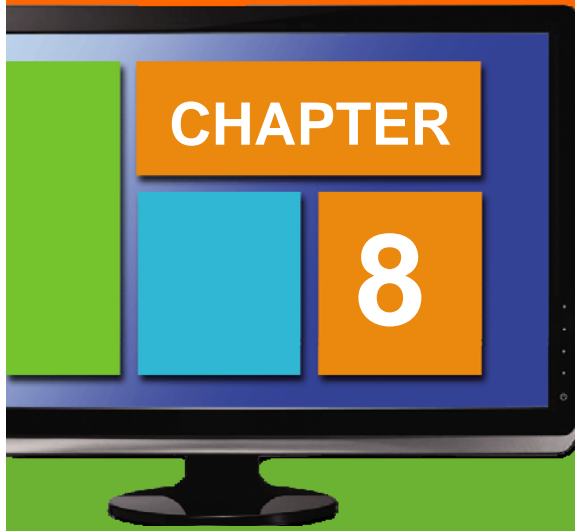
Specifying Temporary Internet File Caching



- Temporary Internet Files consume hard disk space, but help pages load faster.
- Choose Tools, Internet Options, and click the General tab.
- Click Settings under Browsing History, make the desired changes, and click OK.

Checkpoint

- What feature enables you to browse without browsing information being stored?
- What are cookies and what security risk do they pose?
- Why clear the history and other information?
- What is the drawback of deleting temporary Internet files?



Protecting the System with Windows Firewall

Understanding Windows Firewall

- A port is a numbered software channel that directs network input and output, like outgoing and incoming e-mail.
- An unused port can be exploited by malicious software.
- Firewall software blocks port access requested by unknown programs, allowing only specified programs to get through.
- Windows Firewall is turned on by default.

Starting Windows Firewall

- To check Windows Firewall status, open the Control Panel and click System and Security. Click Check Firewall Status.

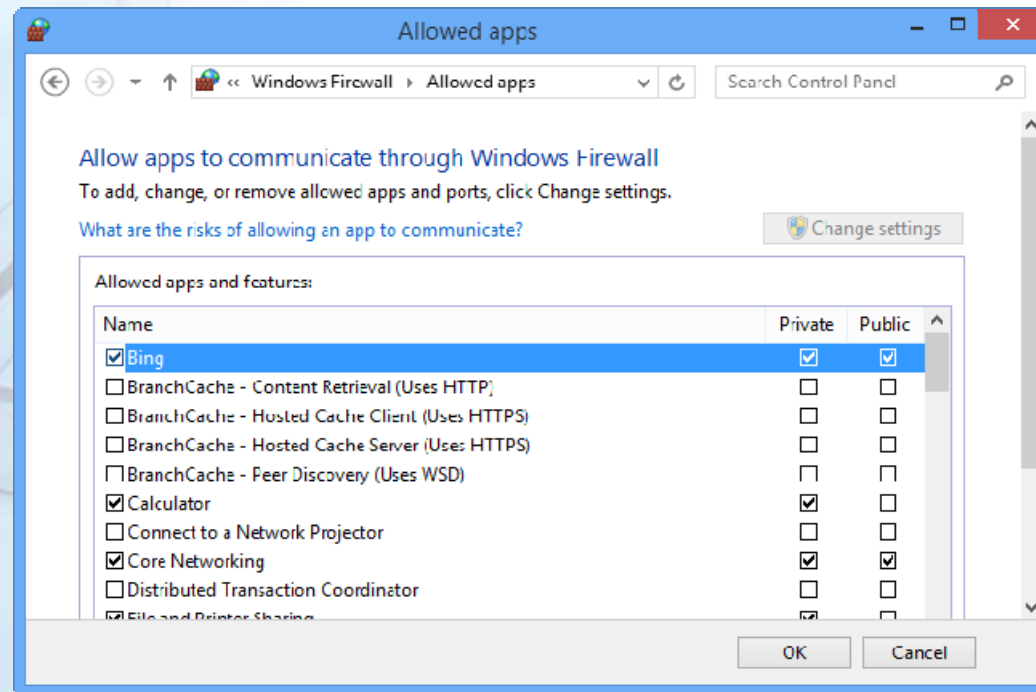


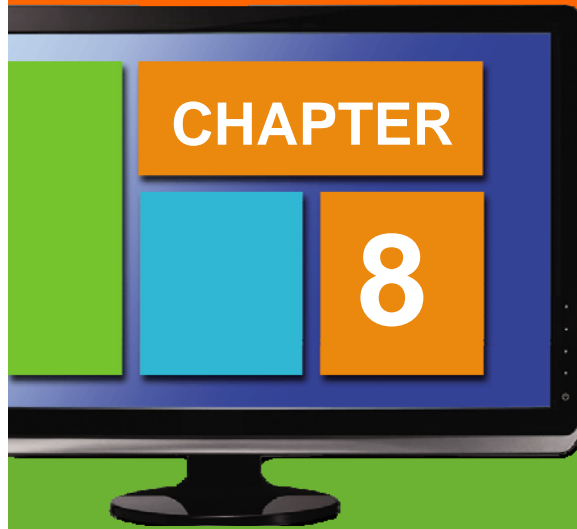
Allowing a Program Through Firewall

- Creating an exception specifically allows a program access through Windows Firewall.
- To create an exception:
 1. Open the Control Panel and click System and Security.
 2. Under Windows Firewall, click Allow a program through Windows Firewall.
 3. Click Change Settings.

Allowing a Program Through Firewall

4. Click applicable check boxes beside a program in the list to allow it or prevent it from connecting.





Protecting Against Viruses and Other Malware with Windows Defender

Understanding Windows Defender

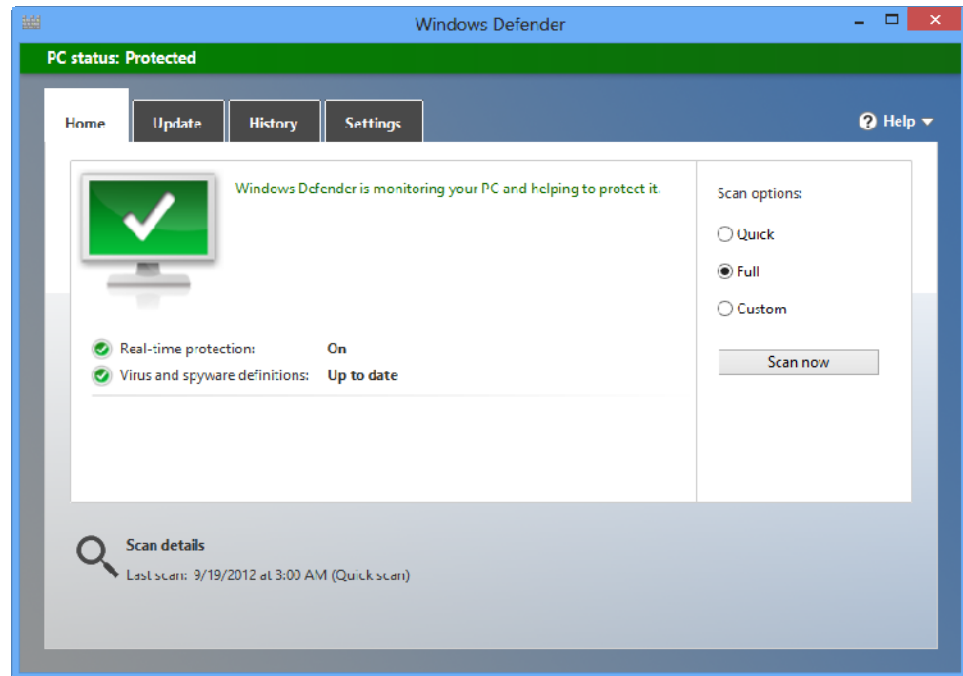
- Windows Defender protects the system against malware, including spyware that collects information and adware that displays ads or redirects IE.
- Windows Defender offers two types of protection:
 - Manually-initiated malware scan.
 - Real-time protection that notifies you if potentially unwanted software tries to install itself or run.
- Use Windows Update to download the latest threat definitions.

Starting Windows Defender

- Control Panel method:
 1. From the Control Panel, in the upper right corner, click Category and then click Large Icons.
 2. Click Windows Defender.
- Start screen method:
 1. Display the Start screen.
 2. Right-click and then click All Apps.
 3. Click Windows Defender.

Scanning the System with Defender

- Windows Defender can perform a quick, full, or custom scan.
- To perform a full scan, click the Full option button and then click Scan Now.

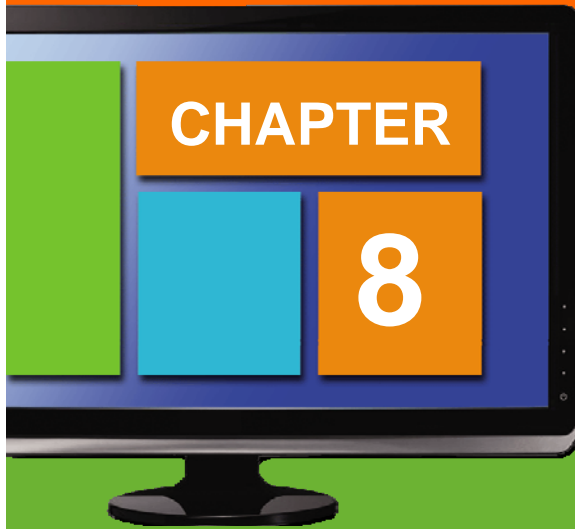


Dealing with Identified Threats

- Windows Defender classifies the threats it finds. Installing Low threat software is usually OK. Software with a higher alert level should be blocked or deleted.
- Windows Defender warns you when an attack is occurring. Use Remove All to remove the threat or Review to get more information.

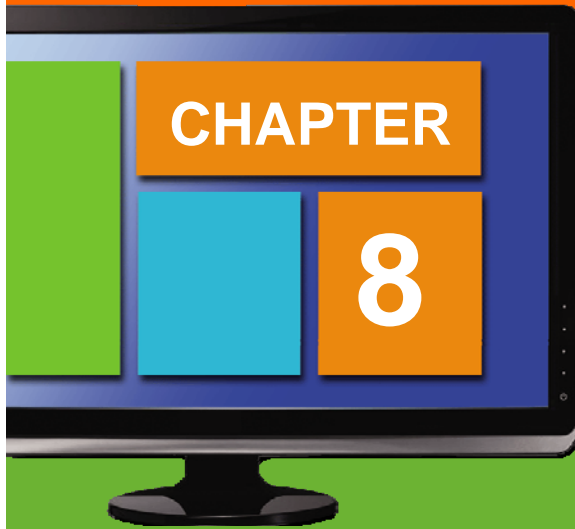
Checkpoint

- What is a port and why must ports be protected for security?
- How do you enable Windows Firewall if needed?
- What is it called when you allow a program through the firewall?
- What does Windows Defender scan for?
- What should you do when Defender identifies a High or Severe alert?



Wrap Up

- Check system security status in Windows Action Center.
- Configure security in IE for four different Internet security zones.
- Stop pop-ups by enabling the Pop-up Blocker.
- Browse safer with InPrivate Browsing.
- Delete and block cookies to protect logon information.



Wrap Up

- Clear history and temporary Internet files for security and to save space.
- Windows Firewall blocks port access requested by unknown programs.
- Windows Defender scans and protects against malware programs.