

Real-World Scenario 5-3: Securing Web Browsers

Scenario: Your organization uses Internet Explorer as its main web browser. Your job as the security administrator is to secure Internet Explorer in as many ways as possible.

Take a look at the configuration settings for your version of IE. Write down some of the ways in which IE can be secured.

(Optional) Take a look at any other browsers you might have running (Firefox, Chrome, Edge, Safari, etc.) and define the types of security they have as well.

Real-World Scenario 5-3 Solution

Internet Explorer can be secured in many ways. The first thing you might do is update to the newest version (if your organization's policy permits) and make sure that version is fully patched. Test the new version thoroughly before deployment. Otherwise, the following is a short list of some of the best ways to secure the browser:

- Turn on automatic website checking with the phishing filter or SmartScreen filter.
- Increase the security of the browser's "zones," such as the Internet zone.
- Increase security for cookies.
- Empty temporary Internet files on exit.
- Set up whitelisting and blacklisting by configuring trusted and restricted websites.
- (Optional) Set up a proxy connection.

Video Solution: Watch the video solution "5-3: Securing Web Browsers."

Simulation: Complete the simulation "5-3: Securing Web Browsers."