

# SOPHOS

## Sophos Endpoint Security and Control Windows XPe/Windows Embedded Standard test guide

Product version: 9.0

Document date: September 2009



# Contents

1 About this guide.....	3
2 Prepare for testing.....	3
3 Install security software.....	3
4 Test threat detection.....	4
5 Test application control.....	5
6 Test data control.....	6
7 Test device control.....	6
8 Copyright.....	7

## 1 About this guide

This guide is for network administrators who want to protect computers running Windows XP Embedded (Windows XPe) or Windows Embedded Standard.

Embedded versions of Windows can be compiled with many different customizations, so this guide does not attempt to discuss whether each can be protected successfully. Instead, it tells you how to run checks after installation to see whether Sophos security software is functioning properly.

This guide assumes that you have previously used Sophos Enterprise Console for installing and managing Sophos software on your network.

It describes how to:

- Install Sophos security software on computers running Windows XPe/Windows Embedded Standard.
- Test that the software is being updated.
- Test threat detection.
- Test application, data and device control.

**Important:** If you complete all the tests in this guide successfully, we will make commercially reasonable efforts in accordance with Sophos's standard business practices to provide technical support. For details, see Sophos support knowledgebase article 63797 (<http://www.sophos.com/support/knowledgebase/article/63797.html>).

## 2 Prepare for testing

Before you start:

- Select endpoint computers running Windows XPe/Windows Standard Embedded to use as test computers.
- Ensure that you have the EICAR virus detection test file installed or ready to install on your test computers.
- Ensure you have MSN Messenger Live available to install on the test computers during application control testing.

## 3 Install security software

Before testing, you need to:

- Install the security software on test computers.
- Check that the software is being updated.

## 3.1 Install software

You install Sophos Endpoint Security and Control 9.0 for Windows in the same way that you would install it on any other Windows endpoint computer.

You can do either of the following:

- **Automatic installation.** In Enterprise Console, find the test computers and ensure they have a valid updating policy. Select the computers, right-click and click **Protect computers**.
- **Manual installation.** At the test computers, browse to the folder from which endpoint computers update and run the Sophos installation program.

Note: The folder from which computers update can be found by looking in **Bootstrap Locations** in Enterprise Console.

## 3.2 Check updating

You should check that the test computers are receiving Sophos updates.

At the test computers:

1. On the taskbar, right-click the Sophos icon and select **Update now**. Wait for the update to be completed.
2. Open Sophos Endpoint Security and Control.
3. On the home page, in the **Status** panel check that the **Last Updated** time has changed.

# 4 Test threat detection

## 4.1 Check that detection works

To check that Sophos Endpoint Security and Control can detect threats, perform an EICAR test as follows.

1. On the test computers, attempt to copy an EICAR test file onto the computer (or to run EICAR if it is already on the computer).

The test computers should display a virus alert.

2. Check that the test computers show the EICAR file in the Quarantine manager and that the details are correct.

## 4.2 Check alerts

Go to Enterprise Console and do as follows:

1. Check that the tabs in the computer list view show the virus name, location and time of discovery.
2. Check that the computer details for the test computers show the correct details.

Now you must clear the alerts.

## 4.3 Clear alerts

1. On the test computers, clear the alert from the Quarantine manager.
2. In Enterprise Console, clear the alert in the **Resolve Alerts and Errors** dialog.

# 5 Test application control

## 5.1 Configure application control

1. In Enterprise console, open an application control policy.
2. Configure the policy to block MSN Live Messenger.
3. Apply the policy to the test computers.
4. In Enterprise Console, check that the policy change is being applied, and that the test computers comply with the policy.

## 5.2 Check that application control works

1. On the test computers, right-click the SESC icon and select Update now.
2. Attempt to install and open MSN Live Messenger.
3. Check that an alert is shown. The application should be shown in the Quarantine manager and all details should be correct, including type.
4. In Enterprise Console, check the computer list view and computer details page.

## 5.3 Clear alerts and reset policy

1. On the test computers, clear the alerts from the Quarantine manager
2. In Enterprise Console, change the application control policy back to its original setting.
3. Check that the endpoint and console comply with the policy change.

## 6 Test data control

### 6.1 Configure data control

1. In Enterprise Console, create a data control policy and open it.
2. On the **Policy Rules** tab, click **Manage rules**.
3. In the **Data Control Rule Management** dialog box, click **Add Content Rule**.
4. Enter a Rule name. Under **Rule Content** click the link in "Where the file contains".
5. In the **Content Control List Management** dialog box, select a CCL and click **OK**.
6. Under **Rule Content**, click the "Select destination" link and check **Removable Storage**. Click **OK**.
7. On the **Data Control Rule Management** dialog box, select the rule you created and click **OK**.
8. Close all dialogs and apply the policy to the test computers.

### 6.2 Check that data control works

1. On the test computers, open Sophos Endpoint Security and Control.
2. On the home page, in the **Status** panel, check that data control is shown as enabled.
3. Click the **Data control log** icon. Check that data control scanning has started.

## 7 Test device control

### 7.1 Configure device control

1. In Enterprise Console, open a device control policy.
2. Configure the policy to block **Modems** and **Wireless**.  

In the Computer details, the Device Control Policy Compliance column should show "Awaiting policy transfer" and then "Same as policy".
3. Apply the policy to the test endpoint computers.
4. Check that the endpoint is now compliant with the policy.

## 7.2 Check that device control works

1. On the endpoint computers, connect modem & wireless devices.  
A balloon warning should be displayed for each blocked device
2. Open Sophos Endpoint Security and Control. On the home page, click the **Device control log** and check that the device is blocked.
3. Check that the Windows Device Manager shows that the device has been disabled.
4. Use the wireless device to attempt to contact a wireless network  
Windows should show that the device is blocked and cannot detect networks.
5. Use the Windows Device Manager to test the modem device. Check that the modem cannot be tested.

## 7.3 Reset device control policy

1. In Enterprise Console, set the device control policy as follows:
  - Modem: Full access.
  - Wireless: Full access.
2. Apply the policy to the test computers.
3. Check that the computers comply with the policy.
4. On the test computers, click the **Device control log** icon and check that the device is enabled.
5. On the endpoint, check that the wireless device can detect wireless networks.
6. Use the Windows Device Manager to test the modem device. Check that the device self test is successful.

## 8 Copyright

Copyright © 2009 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL),

which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to [support@sophos.com](mailto:support@sophos.com) or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>