

# ESM Security Response Policies Release Notes

Nimda response policy  
for Windows NT and Windows 2000



# Nimda NT-W2K ESM Security Response Policies Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

## Copyright Notice

Copyright © 2001 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

**NO WARRANTY.** The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

## Trademarks

Symantec, the Symantec logo, and Enterprise Security Manager are trademarks of Symantec Corporation.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. CERT and CERT Coordination Center are registered trademarks of Carnegie Mellon University.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.





# Nimda NT-W2K ESM Security Response Policy Release Notes

This document contains release notes for the Nimda NT-W2K security response policy for Enterprise Security Manager™ (ESM) Agents on Windows NT and Windows 2000 operating systems.

The Nimda NT-W2K security response policy checks Windows NT 4.0 workstations and servers, and Windows 2000 professional systems and servers, to determine whether these systems are infected by or vulnerable to the W32.Nimda.A@mm worm.

## Introducing security response policies

ESM's security response policies are configured by members of the Symantec Security Response team to respond to recent security incidents and newly-detected security vulnerabilities without waiting for scheduled module Security Update releases.

Security response policy names are identified and sorted by "R-" prefixes in the Policies branch of the ESM Enterprise tree in the ESM Console.

## Nimda NT-W2K policy

The Nimda NT-W2K security response policy identifies Windows NT 4.0 and Windows 2000 systems that are vulnerable to and/or infected by the W32.Nimda.A@mm worm.

W32.Nimda.A@mm is a worm that propagates itself to servers and desktop computers through multiple means. The worm sends itself out by email, exploits open network shares, spreads through Web browsers, and exploits Microsoft Web servers.

When the worm arrives by email, it exploits the MIME header vulnerability in Internet Explorer 5.0.1, 5.5, and previous versions, which allows a virus to be executed simply by reading or previewing a file. The worm also exploits the directory traversal vulnerability on IIS Web servers and prompts Internet Explorer users to download email files with attachments that contain the Nimda virus on compromised Web servers.

For more information about the W32.Nimda.A@mm worm, see the Symantec Code 4 Security Alert at <http://securityresponse.symantec.com>.

## How ESM identifies vulnerable Windows NT and Windows 2000 systems

The Nimda NT-W2K security response policy uses five different ESM modules to identify Windows NT and Windows 2000 systems that are vulnerable to or infected by the W32.Nimda.A@mm worm.

### ■ OS Patches module

The OS Patches module enables nimda.\* template files to check your Windows NT and Windows 2000 systems for Microsoft patch Q290108, "Incorrect MIME header vulnerability," which was released in February, 2001. The module identifies systems that are running this patch by looking at the file date of the Shdocvw.dll file.

If you are running Internet Explorer 5.0.1, 5.5, or previous versions and you have not installed patch Q290108, your systems are vulnerable to the W32.Nimda.A@mm worm.

- **Registry module**

The Registry module enables mime.\* template files to determine whether File Download is enabled in the four Internet Explorer security zones on your Windows NT and Windows 2000 systems. The module returns Red-level security messages for systems with File Download enabled . This represents a critical security threat only on systems that are not installed with patch Q290108. However, Symantec recommends that you disable File Download to protect your systems from future security threats.

- **File Attributes module**

The File Attributes module enables nimda.\* template files to check your Windows NT and Windows 2000 systems for the c:\Admin.dll file. The presence of this file indicates that your systems have been infected by the Nimda virus. Download the Symantec W32.Nimda.A@mm Removal Tool from <http://securityresponse.symantec.com/> and run this utility to remove the worm and restore damaged files.

- **Account Integrity module**

The Account Integrity module generates a list of groups that the Guest account belongs to on your Windows NT and Windows 2000 systems. If this list indicates that the Guest account is a member of the Administrators group or any other privileged group, your systems may have been infected by the Nimda virus. Symantec recommends that you disable the Guest account and remove it from all groups.

- **Network Integrity module**

The Network Integrity module examines your Windows NT and Windows 2000 systems to identify shared directories that give Full Control to the Everyone group. Remove the Everyone group from the access lists for any reported directories and review all network shares to identify any that can be removed.

## How ESM best practice policies can increase your security

Because the W32Nimda.A@mm.worm exploits known vulnerabilities in IIS 4 and IIS 5, Symantec recommends that you also run ESM's IIS best practice policies on your Microsoft Web servers.

## Policy installation procedures

The Nimda NT-W2K ESM security response policy should be installed on ESM Managers that will run the policy on Windows NT and/or Windows 2000 Agents.

---

**Note:** If you intend to run this security response policy on both Windows NT and Windows 2000 Agents, these Agents should have been registered to the Manager before you install the security response policy.

---

## Installation prerequisites

Before you run the executable program that installs the security response policy that is documented in these Notes, you must complete the following prerequisites:

- Upgrade all ESM Manager and Agent systems that will use the security response policy to ESM version 5.1 or later.
- Upgrade the modules on all ESM Manager and Agent systems that will use the security response policy to Security Update 8 or later.

---

**Note:** Make sure you do not modify any of the .option title lines in the SU8 .m (dot-m) files. The security response policy will not recognize edited security check titles.

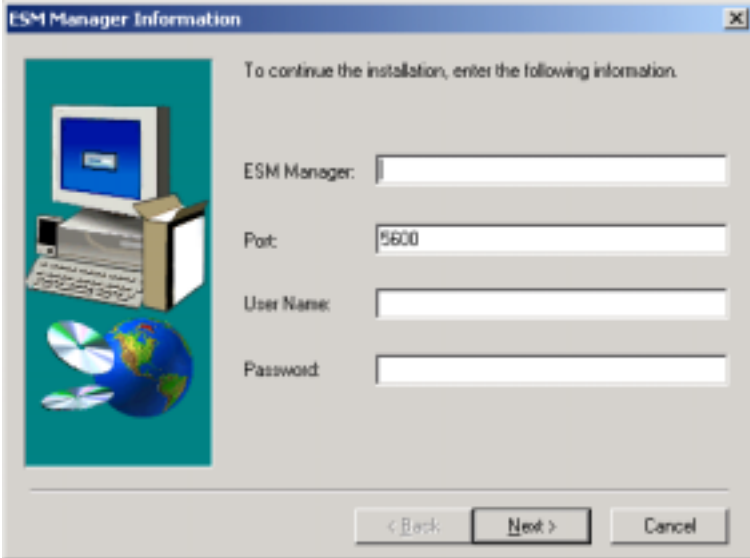
---

- Download the Nimda NT-W2K ESM Security Response policy from <http://securityresponse.symantec.com>.
- Identify the ESM account name, the ESM account password, and the communication port that you will need to use to connect to each ESM Manager you intend to install.

## Installation steps

- 1 Run the Response\_Windows NT - W2K\_Nimda.exe executable file from a system that has network access to the ESM Manager you want to install.
- 2 Click **Next** to close the InstallShield Welcome dialog box.

- 3 If the installation program does not find the required Java™ 2 Runtime libraries on your system, you will be prompted to install the Java 2 Runtime Environment. Click **Yes** to start the installation, click **Yes** to accept the Software License Agreement, and then click **Next** to install the Java 2 Runtime Environment.
- 4 Click **Yes** to continue installation of the security response policy.



ESM Manager Information

To continue the installation, enter the following information.

ESM Manager:

Port:

User Name:

Password:

< Back   Next >   Cancel

- 5 Enter requested ESM Manager Information, then click **Next**.

---

**Note:** If ESM does not find an Agent with the required operating system or ESM security update version on the specified Manager, the install program returns an error message and aborts the installation of the security response policy. To resolve this error, register an Agent with the required application and operating system and install the latest module security update; then rerun the install program.

---

- 6 Click **Finish** to exit the installation program after a successful installation.

## Known restrictions

### Registration of new Agents to ESM Managers that are running security response policies

When you register an Agent with an operating system that was not registered to your ESM Manager before you installed a security response policy, the new Agent's operating system inaccurately displays in the policy's expanded module lists in the ESM Enterprise tree.

For example, if you install the Nimda NT-W2K security response policy on a Manager to which only Windows NT Agents are registered, then register a Windows 2000 Agent to that Manager, the WIN2000 Agent listing will display in the module lists, but the Windows 2000 modules will not execute properly. Reinstall the security response policy to install the Windows 2000 modules.

If you register a UNIX Agent to an ESM Manager where this policy was previously installed, you will also see a UNIX Agent listing in the module lists. This is misleading, because this policy does not run on UNIX Agents. Reinstall the security response policy to correct the module listings.

These are cosmetic errors that will be fixed in the next ESM Console release. In the meantime, remember that each ESM security response policy is intended to run only on ESM Agents that are running the applications and operating system versions that are specifically threatened by described security incidents or vulnerabilities.

# S U P P O R T

## Service and support solutions

Symantec's Technical Support Group of skilled Technical Engineers can provide platform-specific information about Symantec products. Our staff has in-depth expertise in both client/server computing and information security technology.

### Contacting Technical Support

To contact Symantec's technical support:

#### North America, Latin America, or Asia Pacific

Telephone:**(888) 727-8671**

Web:<http://www.symantec.com/techsupp/>

#### Outside North America but supported from the United States (i.e., APLA)

Telephone:**(781) 663-2686**

Web:<http://www.symantec.com/techsupp/>

#### Europe, Middle East, Africa, (EMEA)

Telephone:**+44 (0) 1372 214321**

FAX:**+44 (0) 1372 751815**

**E-mail:**[eurbox\\_epsom@symantec.com](mailto:eurbox_epsom@symantec.com)

## Licensing

Telephone: **(888) 584-3925**

FAX: (781) 487-9818

**E-mail:** [license@symantec.com](mailto:license@symantec.com)

## World Wide Web Site

Web: <http://www.symantec.com/techsupp/>

---

## Service and support offices

### North America

Symantec Corporation  
175 W. Broadway  
Eugene, OR 97401  
U.S.A.

<http://www.symantec.com/>  
Fax: (541) 984-8020

Automated Fax Retrieval

(800) 554-4403  
(541) 984-2490

### Argentina, Chile, and Uruguay

Symantec Region Sur  
Cerrito 1054 - Piso 9  
1010 Buenos Aires  
Argentina

<http://www.symantec.com/region/mx>  
+54 (11) 4315-0889  
Fax: +54 (11) 4314-3434

### Asia/Pacific Rim

Symantec Australia Pty. Ltd.  
408 Victoria Road  
Gladesville, NSW 2111  
Australia

[http://www.symantec.com/region/reg\\_ap/](http://www.symantec.com/region/reg_ap/)  
+61 (2) 9850 1000  
Fax: +61 (2) 9817 4550

### Brazil

Symantec Brasil  
Market Place Tower  
Av. Dr. Chucri Zaidan, 920  
12° andar  
São Paulo - SP  
CEP: 04583-904  
Brasil, SA

<http://www.symantec.com/region/br/>  
+55 (11) 3048-7515  
Fax: +55 (11) 3048-7510

### Colombia, Venezuela, the Caribbean, and Latin America

Symantec Corporation  
175 W. Broadway  
Eugene, OR 97401  
U.S.A.

<http://www.symantec.com/region/mx/>  
+1 (541) 334-6054 (U.S.A.)  
Fax: (541) 984-8020 (U.S.A.)

### Europe, Middle East, and Africa

Symantec Customer Service Center      [http://www.symantec.com/region/reg\\_eu/](http://www.symantec.com/region/reg_eu/)  
P.O. Box 5689      +353 (1) 811 8032  
Dublin 15      Fax: +353 (1) 811 8033  
Ireland

Automated Fax Retrieval      +31 (71) 408-3782

### Mexico

Symantec Mexico      <http://www.symantec.com/region/mx>  
Blvd Adolfo Ruiz Cortines,      +52 (5) 661-6120  
No. 3642 Piso 14  
Col. Jardines del Pedregal  
Ciudad de México, D.F.  
C.P. 01900  
México

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

October 2000