

Symantec NetRecon 3.6
Security Update 2
Release Notes



Symantec NetRecon Security Update 2 Release Notes

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

Documentation version: v3.6 SU2

Copyright Notice

Copyright © 2003 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, Symantec Enterprise Security Manager, LiveUpdate, and Symantec Security Response are trademarks of Symantec Corporation.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other product names that are 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.

Technical support

As part of Symantec Security Response, the Symantec Global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
 - Error messages/log files
 - Troubleshooting performed prior to contacting Symantec
 - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

SYMANTEC NETRECON SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION, AND/OR ITS SUBSIDIARIES ("LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "I DO AGREE" OR "YES" BUTTON OR LOADING THE PRODUCT, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITION, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON AND DO NOT USE THE SOFTWARE.

1. License to Use. Licensor grants You a non-exclusive and non-transferable license (the "License") to use the number of licenses authorized by Your license key of Licensor's software in machine readable form and accompanying documentation (the "Product") on Your computer systems or those authorized by Licensor. The License governs any releases, revisions or enhancements to the Product, which Licensor may furnish to You. You may use Product only to scan networks and computer systems for security-related information to detect actual and potential security flaws and vulnerabilities. You may use the Product only to scan or test computer networks, systems or devices owned by You or which You have express permission to access that you have sufficiently backed-up in case of damage caused by this Product. MISUSE OF THE PRODUCT OR DATA GENERATED BY THE PRODUCT IS STRICTLY PROHIBITED BY LICENSOR, MAY VIOLATE U.S. AND OTHER LAWS AND MAY SUBJECT YOU TO SUBSTANTIAL LIABILITY. You are solely responsible for any misuse of the Product Licensed under this Agreement, and You agree to indemnify Licensor for any liability or damage related in any way to Your use of the Product in violation of this Agreement or the rights of any owner or operator of a computer network, system or device. You are also responsible for using the Product in accordance with the limitations of the license You acquired. The types of licenses are as follows: 1) Evaluation License: You may scan an unlimited number of network resources from one system. Each scan is limited to ten minutes unless otherwise authorized by Licensor, and the evaluation license expires in fifteen days unless otherwise authorized by Licensor. 2) Limited License: You may scan Your small network (up to 254 unique network resources) from one system. 3) Unlimited License: You may scan Your large network (an unlimited number of network resources) from one system. 4) Consultant License: You may scan multiple networks belonging to Your customers as long as permission is obtained before such scan, but such scan shall last for no longer than seven days per customer and Product must be removed thereafter. 5) Not For Resell (NFR) License: You may scan multiple networks belonging to Your customers so long as permission is obtained before such scan, but such scan shall last for no longer than fifteen minutes per customer and Product must be removed thereafter. 6) Single Engagement (SE) License: You may scan multiple networks belonging to a single customer for no longer than thirty (30) days. This license is good for use on one of Your customers only and you must obtain permission before any scan is performed. Such scan may only be for delivering assessment services. You will indemnify and hold Licensor harmless for any claims arising out of the use of Product on machines belonging to any of Your customers or any third party that has been provided access to Product or is scanned by You, except to the extent those claims arise out of Licensor's breach of this license.

2. Restrictions. The Product is owned by Licensor, contains valuable trade secrets of Licensor and is protected by copyright, trademark and trade secret laws and international treaties. You agree to use Product only for Your business purposes, and You agree not to provide any other person with a copy of, or access to, any part of Product unless authorized by Your type of license. You may make one copy of Product for back-up, archive or disaster recovery purposes. You may only make copies of documentation as needed for Your internal use of the Product. Each copy of any part of the Product made by or for You must contain all of Licensor's proprietary markings and copyright notices without alteration. You may not sell, transfer, sublicense, lend, or rent Product to any other person or allow any other person to use Product for any reason, including by making it available for timesharing, service bureau or on-line use. Use by persons to which You have contracted any of Your data processing services is permitted only if each contractor (and its associated employees) is subject to a valid written agreement prohibiting the reproduction or disclosure to other persons of software products and associated Documentation to which they have access and such prohibitions apply to Product. You may not decompile, disassemble, reverse engineer, modify or attempt to discover the source code of Product except as expressly permitted by the laws of the jurisdiction in which You are located, and You may not copy, transfer, or otherwise use Product except as expressly permitted by this license. Use of Product in conjunction with any software product that decompiles or recompiles the Product or in any way creates a derivative or modified copy of Product is an unauthorized use and is prohibited.

3. Limited Warranty. Licensor will replace, at no charge, defective media and product materials that are returned within 30 days of shipment. Licensor warrants, for a period of 30 days the shipment date, that Product will perform in substantial compliance with the written materials accompanying the Product on that hardware and operating system software for which it was designed, as stated in the documentation. Use of Product with hardware and/or operating system software other than that for which it was designed and voids this applicable warranty. If, within 30 days of shipment, You report to Licensor that Product is not performing as described above, and Licensor is unable to correct it within 30 days of the date You report it, You may return Product, and Licensor will refund the License fee. If You promptly notify Licensor of an infringement claim based on an existing U.S. patent, copyright, trademark or trade secret, Licensor will indemnify You and hold You harmless against such claim, and shall control any defense or settlement. This warranty is null and void if You have modified Product, combined the Product with any software or portion thereof owned by any third party that is not specifically authorized or failed promptly to install any version of Product provided to You that is non-infringing. If commercially reasonable, Licensor will either obtain the right for You to use the Product or will modify Product to make it non-infringing. The remedies above are Your exclusive remedies for Licensor's breach of any warranty contained herein.

4. Limitation of Remedies. You understand that the operation of Program may cause problems on or failures of computer networks, systems and devices, which may result in loss of data, unavailability of computing resources or other damage. You represent to Licensor that You own or are authorized to use Product on any computer networks, systems or devices on which Product may be used or that may be tested by Product, You accept all risk of any such damage or loss, any You hereby waive all rights, remedies and causes of action that may arise therefrom. IN NO EVENT WILL LICENSOR OR ITS REPRESENTATIVES BE LIABLE ANY SUCH DAMAGES OR LOSSES WHATSOEVER, INCLUDING ANY LOSS OF PROFITS, LOST

SAVINGS, LOSS OF DATA OR LOSS OF USE OR COMPUTER HARDWARE OR SOFTWARE MALFUNCTION OR OTHER SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF LICENSOR OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES. LICENSOR AND ITS REPRESENTATIVES WILL NOT BE LIABLE FOR ANY LOSSES OR DAMAGES CAUSED BY USE OF THE PRODUCT NOT PERMITTED BY THIS AGREEMENT. IN NO EVENT SHALL LICENSOR'S TOTAL LIABILITY UNDER THIS AGREEMENT EXCEED THE AMOUNT PAID FOR THE PRODUCT. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. No action or claim arising out of or relating to this Agreement may be brought by You more than one (1) year after the cause of action is first discovered.

5. **Confidentiality.** You agree that all information relating to the Product is confidential property of the Licensor ("Proprietary Information"). You will not disclose any Proprietary Information to any third party except to the extent You can document that any such Proprietary Information is in the public domain and generally available for use and disclosure by the general public without any charge or license. If you have obtained a Consultant or NFR license, disclosure to Your clients is permitted only if they have executed a confidentiality agreement that encompasses non-disclosure of Proprietary Information with protections as strict as those contained herein, and such disclosure shall not last longer than allowed by restrictions on use under such license. You recognize and agree that there is no adequate remedy at law for a breach of this section, that such a breach would irreparably harm Licensor and that Licensor is entitled to equitable relief (including, without limitation, injunctive relief) with respect to any such breach or potential breach, in addition to any other remedies available at law.

6. **Export Regulation.** You agree to comply strictly with all US export control laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses to export, re-export or import the Product. These products are prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria or Sudan.

7. **US Government Restricted Rights.** If You are acquiring the Product or its accompanying documentation on behalf of the US Government, it is classified as "Commercial Computer Product" and "Commercial Computer Documentation" developed at private expense, contains confidential information and trade secrets of Licensor and its licensors, and is subject to "Restricted Rights" as that term is defined in the Federal Acquisition Regulations ("FARs"). Contractor/Manufacturer is: Symantec Corporation., and its subsidiaries, Cupertino, CA, USA.

8. **Miscellaneous.** This License is made under the laws of the State of California, USA, excluding the choice of law and conflict of law provisions. This License is the entire License between You and Licensor relating to the Product and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communication between the parties during the term of this License. Notwithstanding the foregoing, some Product or products of Licensor may require Licensee to agree to additional terms through Licensor's on-line "click-wrap" license, and

such terms shall supplement this Agreement. If any provision of this License is held invalid, all other provisions shall remain valid unless such validity would frustrate the purpose of this License, and this License shall be enforced to the full extent allowable under applicable law. No modification to this License is binding, unless in writing and signed by a duly authorized representative of each party. The License granted hereunder shall terminate upon Your breach of any term herein and you shall cease use of and destroy all copies of Product. Any Product purchased by You after the purchase of the Product which is the subject of this License shall be subject to all of the terms of this License. All of Symantec Corporation's and its subsidiaries' licensors are direct and intended third-party beneficiaries of this License and may enforce it against you.

Revision February 21, 2001

Contents

Security Update 2

New vulnerability detection	3
Microsoft Data Access Components RDS Buffer Overflow	3
Microsoft Windows Locator Service Buffer Overflow Vulnerability	4
Microsoft SQL Server SQLXML Buffer Overflow Vulnerability	4
Microsoft SQL Server 2000 SQLXML Script Injection Vulnerability	4
Microsoft SQL Server 2000 lets remote users mount a DoS	4
Microsoft SQL Server 2000 OpenDataSource buffer overflow	4
Sendmail Header Processing Buffer Overflow Vulnerability	4
Vulnerability name changes	5

Security Update 1

New vulnerability detection	6
Microsoft SQL Server 7.0 OLE DB Provider Name Buffer Overflow Vulnerability	6
Microsoft SQL Server 2000 OLE DB Provider Name Buffer Overflow Vulnerability	6
Microsoft SQL Server 7.0 Multiple Extended Stored Procedure Buffer Overflow	6
Microsoft SQL Server 2000 Multiple Extended Stored Procedure Buffer Overflow	6
Microsoft SQL Server 2000 Password Encrypt Procedure Buffer Overflow	6
Microsoft SQL Server 2000 Resolution Service Heap Overflow Vulnerability	6
Microsoft SQL Server 2000 sp_MScoptscript stored procedure validation	7
Microsoft SQL Server 7.0 authentication engine vulnerable to buffer overflow	7
Microsoft SQL Server 2000 authentication engine vulnerable to buffer overflow	7
Microsoft SQL Server 2000 Resolution Service Stack Overflow Vulnerability	7
Command line interface (CLI) enhancements	8
License key	8
Symantec NetRecon data (.nrd) files	8

Release Notes

The contents of Security Update 2 (SU2) for Symantec NetRecon 3.6 can be installed only through LiveUpdate (Click **LiveUpdate** on the Symantec NetRecon icon bar).

Security Update 2

Symantec NetRecon 3.6 SU2 adds detection and reporting of four Microsoft SQL Server vulnerabilities and the sendmail header processing buffer overflow. Several SQL Server vulnerabilities have also been renamed.

New vulnerability detection

With the addition of SU2, Symantec NetRecon can now detect and report the following vulnerabilities:

- **Microsoft Windows 2000 ntdll.dll Buffer Overflow Vulnerability**
The Windows ntdll.dll system component vulnerable to a buffer overrun when passed data from certain functions; remote code execution is possible. The Windows 2000 library ntdll.dll includes a function that does not perform sufficient bounds checking. The vulnerability is present in the RtlDosPathNameToNtPathName_U function and may be exploited through other programs that use the library if an attack vector permits it. One of these programs is the implementation of WebDAV that ships with IIS. The vector allows for the vulnerability in ntdll.dll to be exploited by a remote attacker.
- **Microsoft Data Access Components RDS Buffer Overflow Vulnerability**
MDAC contains a buffer overflow that could lead to arbitrary code execution in MSIE and on vulnerable IIS servers.

- **Microsoft Windows Locator Service Buffer Overflow Vulnerability**
The Locator service for Windows domain controller systems is prone to a buffer overflow condition. Arbitrary code execution is possible.
- **Microsoft SQL Server SQLXML Buffer Overflow Vulnerability**
Attackers can initiate SQL Server 2000 buffer overflows by connecting to a host through HTTP, then submitting malformed data directly to the SQLXML HTTP component. The overflow condition occurs when an overly long value is given to the contenttype=parameter.
- **Microsoft SQL Server 2000 SQLXML Script Injection Vulnerability**
SQLXML components are prone to script injection attacks via an unchecked parameter in XML tags. Under some circumstances it is possible to inject arbitrary script code in XML tags. This lets an attacker execute script code in the context of the Internet Explorer Security Zone associated with the IIS server running the vulnerable components.
- **Microsoft SQL Server 2000 lets remote users mount a DoS**
SQL Server 2000 lets remote attackers mount a denial of service attack through a malformed 0x08 packet that is missing a colon separator.
- **Microsoft SQL Server 2000 OpenDataSource buffer overflow**
Buffer overflow in the OpenDataSource function of the Jet engine on SQL Server 2000 lets remote attackers execute arbitrary code.
- **Sendmail Header Processing Buffer Overflow Vulnerability**
Buffer overflow in the OpenDataSource function of the Jet engine on Microsoft SQL Server 2000 lets remote attackers execute arbitrary code.
For more information on the sendmail header processing buffer overflow, go to <http://securityresponse.symantec.com/avcenter/security/Content/3.3.2003.html>.

Vulnerability name changes

In SU2 the following Symantec NetRecon vulnerability names are changed:

Table 2-1 Vulnerability name changes

Old name	New name
SQL Server 7.0 Remote Data Source function contains unchecked buffers	Microsoft SQL Server 7.0 OLE DB Provider Name Buffer Overflow
SQL Server 2000 Remote Data Source function contains unchecked buffers	Microsoft SQL Server 2000 OLE DB Provider Name Buffer Overflow Vulnerability
SQL 7.0 extended stored procedures vulnerable to buffer overflow and DoS	Microsoft SQL Server 7.0 Multiple Extended Stored Procedure Buffer Overflow
SQL 2000 extended stored procedures vulnerable to buffer overflow and DoS	Microsoft SQL Server 2000 Multiple Extended Stored Procedure Buffer Overflow
SQL 2000 password encryption procedure vulnerable to buffer overflow attacks	Microsoft SQL Server 2000 Password Encrypt Procedure Buffer Overflow
SQL 2000 Resolution Service allows remote DoS or execution of arbitrary code	Microsoft SQL Server 2000 Resolution Service Heap Overflow Vulnerability
SQL Server 2000 sp_MScopyscript stored procedure fails to validate input	Microsoft SQL Server 2000 sp_MScopyscript stored procedure validation
SQL Server 7.0 authentication engine vulnerable to buffer overflow attacks	Microsoft SQL Server 7.0 authentication engine vulnerable to buffer overflow
Server 2000 authentication engine vulnerable to buffer overflow attacks	Microsoft SQL Server 2000 authentication engine vulnerable to buffer overflow
MSSQL Buffer Overflow vulnerable to W32.Slammer worm attack	Microsoft SQL Server 2000 Resolution Service Stack Overflow Vulnerability

Security Update 1

New vulnerability detection

Note: The names of SU1 vulnerabilities were changed in SU2. The current (SU2+) names are used below. For the names that were used in SU1, see “Vulnerability name changes” on page 5.

- **Microsoft SQL Server 7.0 OLE DB Provider Name Buffer Overflow Vulnerability**
Symantec NetRecon can identify a buffer overflow in Microsoft SQL 7.0 that may let remote attackers execute arbitrary code on the system or gain privileged access to the SQL database.
- **Microsoft SQL Server 2000 OLE DB Provider Name Buffer Overflow Vulnerability**
Symantec NetRecon can identify a buffer overflow in Microsoft SQL 2000 that may let remote attackers execute arbitrary code on the system or gain privileged access to the SQL database.
- **Microsoft SQL Server 7.0 Multiple Extended Stored Procedure Buffer Overflow**
Symantec NetRecon can identify Microsoft SQL Server 7.0 extended stored procedures that fail to validate input correctly, which may allow buffer overflow attacks and denial of service (DoS) attacks.
- **Microsoft SQL Server 2000 Multiple Extended Stored Procedure Buffer Overflow**
Symantec NetRecon can identify Microsoft SQL Server 2000 extended stored procedures that fail to validate input correctly, which may allow buffer overflow attacks and denial of service (DoS) attacks.
- **Microsoft SQL Server 2000 Password Encrypt Procedure Buffer Overflow**
Symantec NetRecon can identify a Microsoft SQL Server 2000 credential encryption procedure that is vulnerable to a buffer overflow attack, which could compromise control of the database and possibly the server. The SQL 2000 Resolution Service may allow remote DoS or execution of arbitrary code.
- **Microsoft SQL Server 2000 Resolution Service Heap Overflow Vulnerability**
Symantec NetRecon can identify the Microsoft SQL Server 2000 Resolution Services that contain multiple vulnerabilities. These vulnerabilities allow

denial of service attacks as well as possible execution of arbitrary code through buffer overflow attacks.

- **Microsoft SQL Server 2000 sp_MScoptscript stored procedure validation**
Symantec NetRecon can identify the Microsoft SQL Server 2000 sp_MScoptscript on network resources. Microsoft SQL Server 2000 fails to validate input, which may allow attackers to execute arbitrary code and gain privileged access to stored procedures in the SQL database.
- **Microsoft SQL Server 7.0 authentication engine vulnerable to buffer overflow**
Symantec NetRecon can identify the authentication engine for the Microsoft SQL Server 7.0. The authentication engine is vulnerable to buffer overflow attacks that may let attackers execute arbitrary code and gain privileged access to the stored procedure, or cause a denial of service for the SQL service.
- **Microsoft SQL Server 2000 authentication engine vulnerable to buffer overflow**
Symantec NetRecon can identify the authentication engine for the Microsoft SQL Server 2000. The authentication engine is vulnerable to buffer overflow attacks that may let attackers execute arbitrary code and gain privileged access to the stored procedure, or cause a denial of service for the SQL service.
- **Microsoft SQL Server 2000 Resolution Service Stack Overflow Vulnerability**
Symantec NetRecon can identify a problem with the Microsoft SQL Server 2000 Resolution Service, which may make it possible for a remote user to execute arbitrary code on a vulnerable host. An attacker could exploit a stack-based overflow in the Resolution Service by sending a maliciously crafted UDP packet to port 1434. A vulnerable version of Microsoft SQL Server 2000 Desktop Engine is automatically installed with Internet Explorer 6 on .NET servers.
- **MSSQL Server detected**
MSSQL Server has been detected.

Command line interface (CLI) enhancements

License key

The Symantec NetRecon command line interface (CLI) can now accept license key information. Four options are required to successfully register the license key using the CLI.

Table -1 License key options

Option	Description
-license [-l]	Specify the Symantec NetRecon license key.
-company [-c]	Specify the company name that is associated with the license.
-serial [-s]	Specify the serial number that is associated with the license.
-type [-t]	Specify the type that is associated with the license.

Note: If an error occurs during the license registration, Symantec NetRecon places an error message in the errors.log file.

Symantec NetRecon data (.nrd) files

You must now use the following options to specify .nrd files in the command line interface.

Table -2 nrd file options

Option	Description
-nrdir [-i]	Specify the .nrd input file.
-nrdir [-o]	Specify the .nrd output file.

Note: It is not necessary to submit .nrd files to change the license. However, if you omit one or both of the .nrd files, Symantec NetRecon will not attempt a scan.

CLI formatting and syntax are fully documented in the Symantec NetRecon online Help system. Users who are not familiar with the CLI should read the entire Use the Command Line Interface (CLI) Help section.

To locate the Help Topic on .nrd files

- 1** On the NetRecon console menu, click **Help**.
- 2** Click **Help Topics**.
- 3** Click the topic labeled **How do I...**
- 4** Click **Use the Command Line Interface (CLI)**.
- 5** Click **Understanding .NRD Files**.

