

Intel[®] vPro[™] Technology Use Case Reference Design

Enhanced Remote Repair - Virus Scan

Revision 1.1

June, 2010

Document ID: 1006

Revision History

Revision	Revision History	Date
1.0	Initial release.	February 2010
1.1	Changed title per Marketing.	June 2010

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

EXCLUSION OF OTHER WARRANTIES. THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the Software.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The Intel® Active Management Technology may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site.

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/

Throughout this document Intel ME refers to Intel® Management Engine and Intel® AMT refers to Intel® Active Management Technology.

Intel, the Intel logo, Intel® AMT, and Intel® vPro™ are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2010 Intel Corporation. All rights reserved.

Contents

Revision History	ii
Contents	iii
1 Preface	5
1.1 Document Scope	5
1.2 Intended Audience.....	5
1.3 Related Documentation	5
2 Introduction	6
2.1 Example Deployment Illustrated in This Document.....	6
2.2 Process Overview	6
2.2.1 Setup.....	7
2.2.2 Remote Virus Scan	7
3 Setup.....	8
3.1 Obtain the Files	8
3.2 Install ClamWin on the Help Desk Console	9
3.3 Copy the EICar Virus Test File to the Target Client.....	13
4 Perform Remote Virus Scan.....	14
4.1 Map a Drive to the Target Client Hard Drive	14
4.2 Perform a Scan and Clean All Found Viruses.....	14

1 Preface

Intel® vPro™ technology provides the ability for the help desk to perform all kinds of remote diagnostics and repair that otherwise would have taken a desk side visit. This Use Case Reference Design (UCRD) will outline how to perform a remote virus scan.

1.1 Document Scope

This document describes a theory and process for performing a remote virus scan. We recommend that you follow the included procedures in your test lab and then adjust the process based on the specific needs of your production environment. Note that the process described in this document assumes you have gained access to the remote system's hard drive using the Remote Drive Share software and procedures (see 1.3, Related Documentation below). Other remote access methods may work with these steps as well, but they have not been tested as part of this document's development. Also, there are other possible methods to perform a remote scan such as a remote IDE-R boot to a virus scanner CD. These are also not covered in this document.

1.2 Intended Audience

This document is intended for Information Technology (IT) professionals who work on, manage, or develop processes for a help desk. Readers should be familiar with Remote Drive Sharing (RDS), as described in the document(s) listed in 1.3, Related Documentation below.

1.3 Related Documentation

The following documents and software are required in order to perform the procedures contained in this Use Case Reference Design.

- UCRD 1040, *Use Remote Drive Sharing to Remotely Access and Repair a PC with Intel® vPro™ Technology*, available at <http://communities.intel.com/docs/DOC-4785>

2 Introduction

2.1 Example Deployment Illustrated in This Document

The steps in this document outline a lab experiment to prove the concept of a remote virus scan. Steps include setting up the lab environment and then running the scan to detect a virus. The lab contains two computers:

Role	Requirement
Help Desk Console	<ul style="list-style-type: none">Any computer with virus scan software. The procedure uses Clam Win.Remote access to the hard drive of Target Client using Remote Drive Sharing.
Target Client with Intel vPro Technology	<ul style="list-style-type: none">Any PC with Intel vPro Technology.

2.2 Process Overview

Once you have gained remote access to the client hard drive many tasks become possible to execute remotely. A virus scan is one of such task. The concept is quite simple: using Remote Drive Sharing, the remote drive is mapped to a drive letter on the Help Desk Console (see 1.3, Related Documentation on page 5). Once remote access is established, a virus scanner resident on the Help Desk Console is executed to scan the mapped drive.



NOTE

Boot Sector viruses will not be detected since the disk's boot sector is not available via Remote Drive Sharing.

This procedure uses an industry standard test file to make the virus scanner think it has detected a virus: http://www.eicar.org/anti_virus_test_file.htm.

Although this file is an inert file containing ASCII text, all virus scanners will detect it as a virus.

2.2.1 Setup

Phase description	The IT professional performs tasks to prepare the Help Desk Console and the Target Client for the lab experiment.
Phase prerequisites	<ul style="list-style-type: none"> You have read, understood, and performed the procedures in UCRD 1040, <i>Use Remote Drive Sharing to Remotely Access and Repair a PC with Intel® vPro™ Technology</i> (see see 1.3, Related Documentation on page 5) Remote Drive Sharing is working in the lab between the Help Desk Console and the Target Client
Phase flow	<ol style="list-style-type: none"> Obtain the files. Install ClamWin. Copy the eicar test file to the client.
Phase outcome	You are ready to perform a remote virus scan.

2.2.2 Remote Virus Scan

Phase description	The IT professional performs a remote virus scan, detects a virus, and cleans the hard drive.
Phase prerequisites	Setup phase was successfully completed.
Phase flow	<ol style="list-style-type: none"> If you have not already done so as part of the setup phase, map a drive letter from the Help Desk Console to the Target Client hard drive. Perform a scan of the mapped drive and clean all found viruses.
Phase outcome	Any virus on the Target Client has been detected and removed. The concept may now be adapted for production use.

3 Setup

This chapter and its subsections describe the process to prepare a Help Desk Console for performing a remote virus scan.



NOTE

Remote Drive Sharing or another method of mapping the Target Client's hard drive to a drive letter on the Help Desk Console must be configured and working. Steps are not covered in this document.

3.1 Obtain the Files

1. Download the latest ClamWin free virus scanner software (Note: any virus scanner should work for this process):

<http://www.clamwin.com>.

As of this writing the latest ClamWin version is 0.95.3.

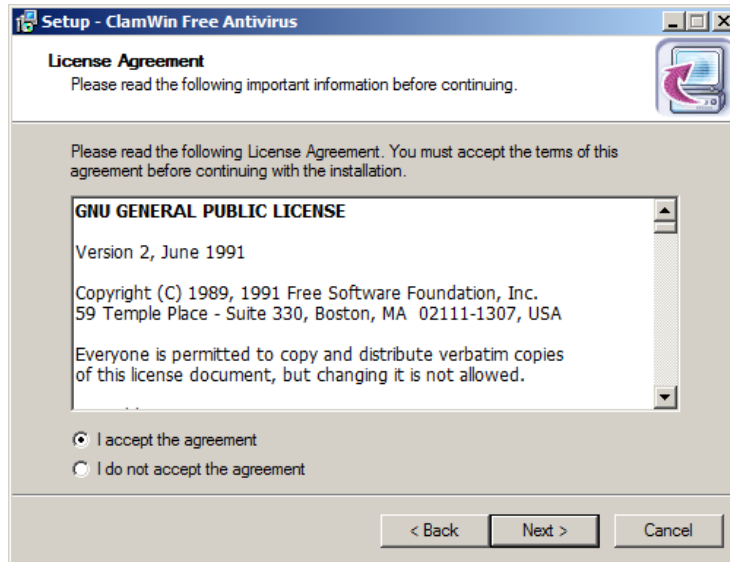
2. Obtain EICAR virus test pattern. You have two options:

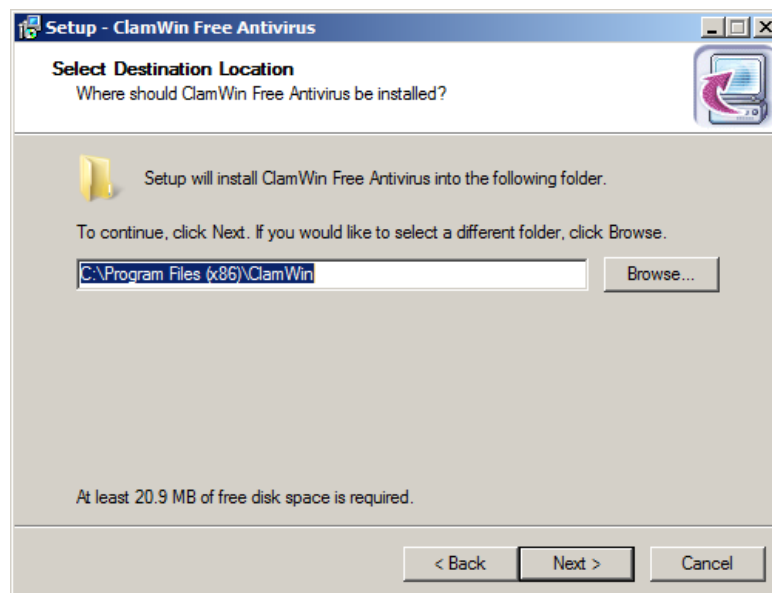
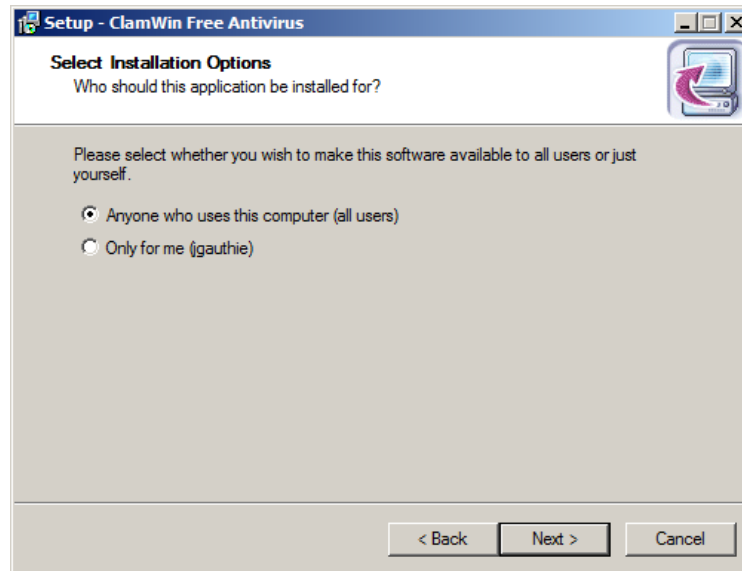
- Download one of the test files from http://www.eicar.org/anti_virus_test_file.htm. This document uses **eicar.com.txt**. Note: if you have a real time virus scanner it will detect this file as a virus. There is no danger. This is a test file only. You must disable real time scanning to interact with this file.
- Create a new text file named eicar.com.txt. Copy the contents below and paste them into the text file:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

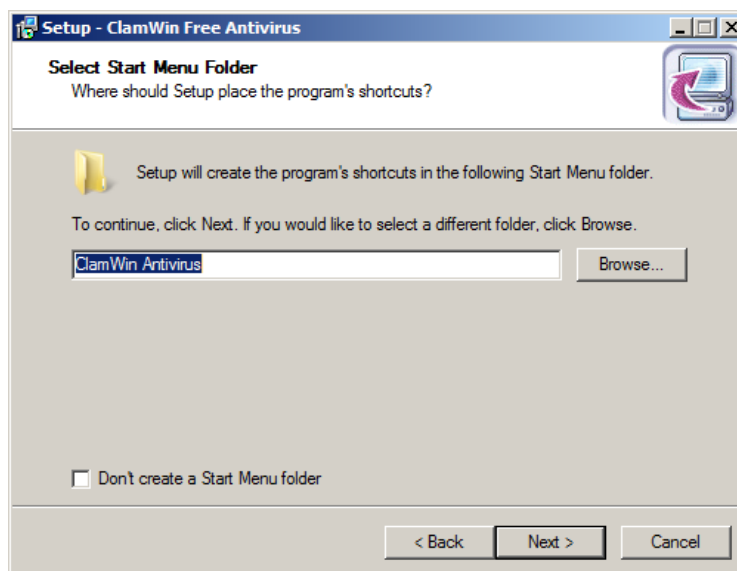
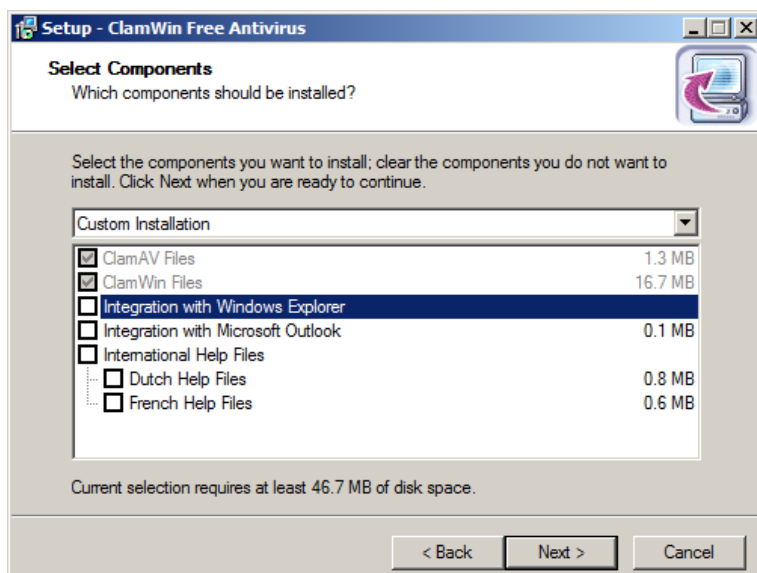

3.2 Install ClamWin on the Help Desk Console

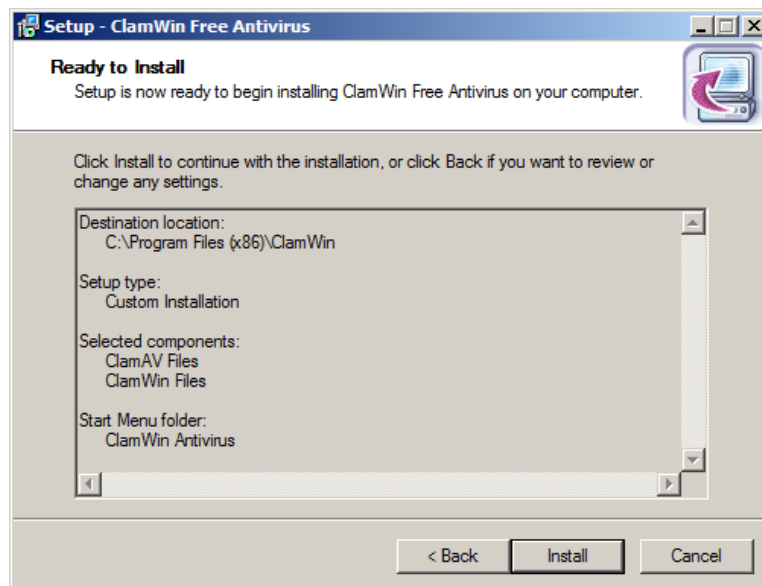
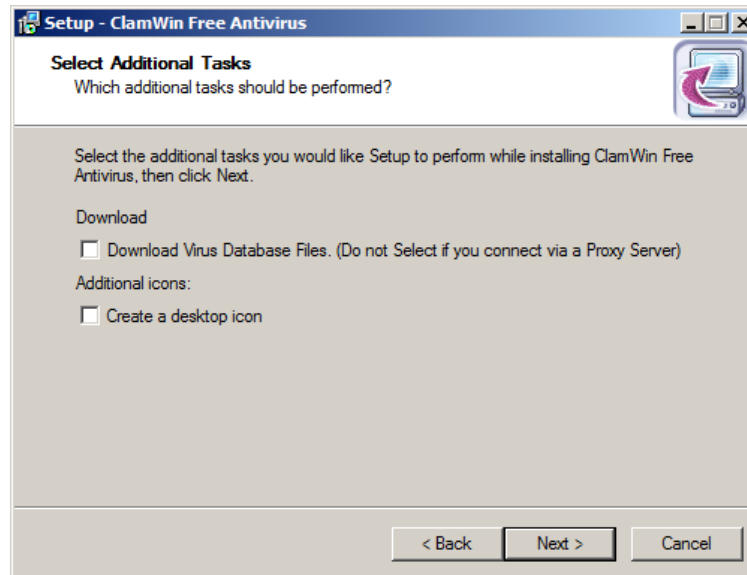
1. Copy the ClamWin installer (clamwin-0.95.3-setup.exe) to the Help Desk console.
2. Run the installer and follow the prompts as outlined below

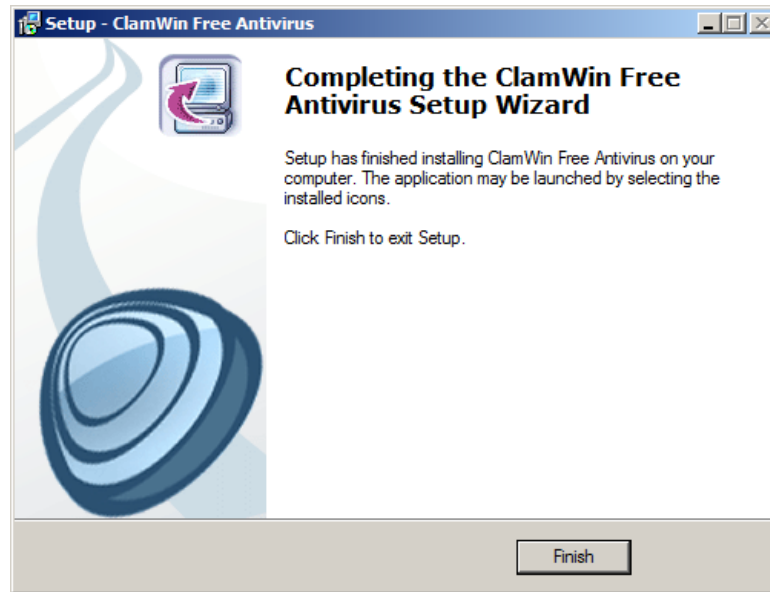




Note: use the default option in the above screen – the location may change based on your OS.







ClamWin is now installed and ready for use.

3.3 Copy the EICar Virus Test File to the Target Client

1. Disable any virus scanner on the target client.
2. Copy the file eicar.com.txt to c:\ of the target client.

4 Perform Remote Virus Scan

This chapter leads you through performing the remote virus scan.

4.1 Map a Drive to the Target Client Hard Drive

If you have not already done so, map a drive letter from the Help Desk Console to the shared hard drive of the Target Client.

- Refer to UCRD 1040, *Use Remote Drive Sharing to Remotely Access and Repair a PC with Intel® vPro™ Technology* (see see 1.3, Related Documentation on page 5).
- The following steps assume the drive letter Q: is mapped to the Target Client's hard drive.



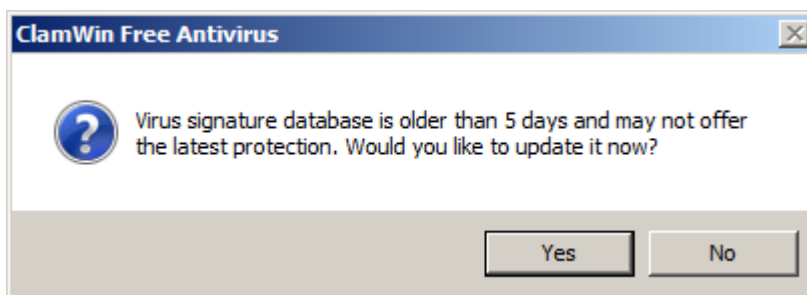
NOTE

Other methods of mapping a remote drive should work as well. If you prefer another method, please perform it now and continue on to the next section.

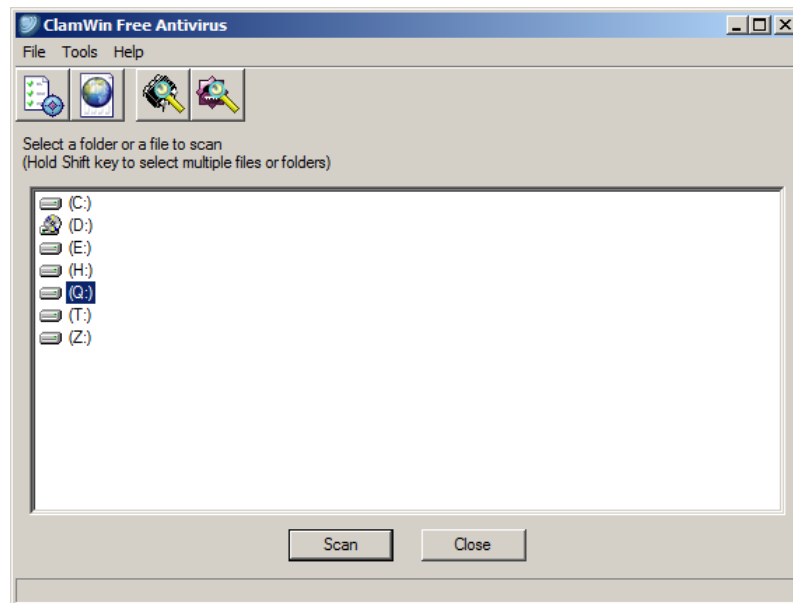
4.2 Perform a Scan and Clean All Found Viruses

On the Help Desk Console, perform the following steps.

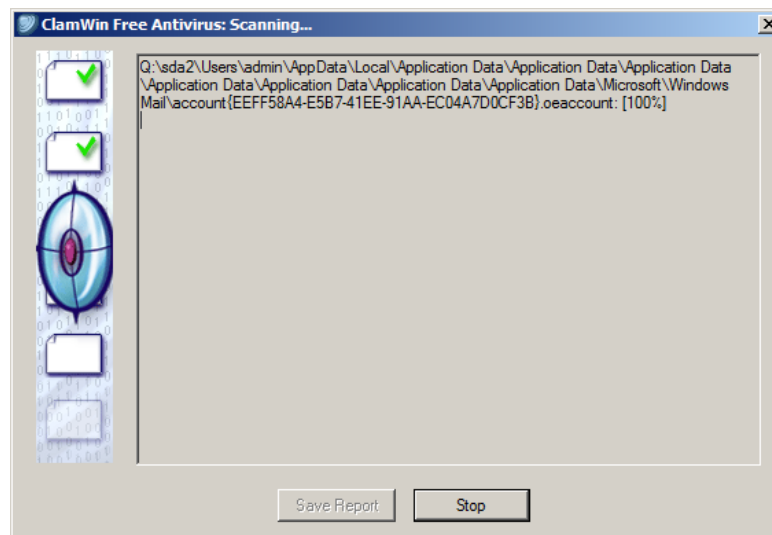
1. Open ClamWin.
2. If prompted to update the virus definitions, click **No** (to save time), since the EICAR test file will be detected using whatever definitions you have already. In production, however, be sure to always update to the latest virus definitions.



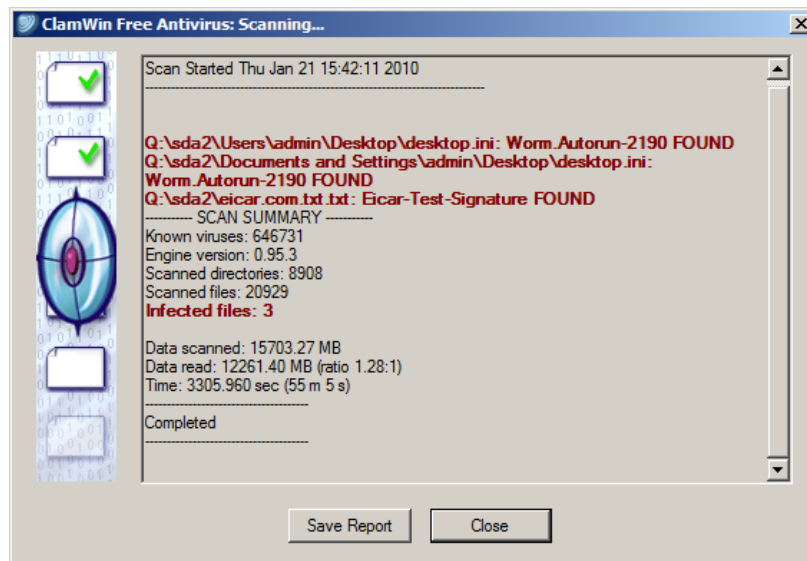
3. Select Drive Q: and click **Scan**.



4. ClamWin scans all files on the Q: drive.



5. When complete, the EICAR test “virus” will be detected.



And that's it. You've just performed a remote virus scan. It's that easy.