

# eTrust™ Vulnerability Manager Director



# Getting Started

## eTrust Vulnerability Manager Director Setup Guide



Computer Associates®

---

This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

THIS DOCUMENTATION MAY NOT BE COPIED, TRANSFERRED, REPRODUCED, DISCLOSED OR DUPLICATED, IN WHOLE OR IN PART, WITHOUT THE PRIOR WRITTEN CONSENT OF CA. THIS DOCUMENTATION IS PROPRIETARY INFORMATION OF CA AND PROTECTED BY THE COPYRIGHT LAWS OF THE UNITED STATES AND INTERNATIONAL TREATIES.

NOTWITHSTANDING THE FOREGOING, LICENSED USERS MAY PRINT A REASONABLE NUMBER OF COPIES OF THIS DOCUMENTATION FOR THEIR OWN INTERNAL USE, PROVIDED THAT ALL CA COPYRIGHT NOTICES AND LEGENDS ARE AFFIXED TO EACH REPRODUCED COPY. ONLY AUTHORIZED EMPLOYEES, CONSULTANTS, OR AGENTS OF THE USER WHO ARE BOUND BY THE CONFIDENTIALITY PROVISIONS OF THE LICENSE FOR THE SOFTWARE ARE PERMITTED TO HAVE ACCESS TO SUCH COPIES. THIS RIGHT TO PRINT COPIES IS LIMITED TO THE PERIOD DURING WHICH THE LICENSE FOR THE PRODUCT REMAINS IN FULL FORCE AND EFFECT. SHOULD THE LICENSE TERMINATE FOR ANY REASON, IT SHALL BE THE USER'S RESPONSIBILITY TO RETURN TO CA THE REPRODUCED COPIES OR TO CERTIFY TO CA THAT SAME HAVE BEEN DESTROYED. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH LOSS OR DAMAGE.

THE USE OF ANY PRODUCT REFERENCED IN THIS DOCUMENTATION AND THIS DOCUMENTATION IS GOVERNED BY THE END USER'S APPLICABLE LICENSE AGREEMENT.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

\* 2003 Computer Associates International, Inc. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

# eTrust™ Vulnerability Manager Director

## To get started, you will need:

1. Network cables and network connectivity
2. Static, available IP Address and Subnet Mask with Internet connectivity
3. IP Address of Default Gateway, DNS and Proxy Servers, with login credentials, if applicable
4. License Key
5. A laptop, PC or server with IE 5.0 or higher installed to access eTrust Vulnerability Manager-Director

## Setup Overview

1. **Plug in network cable** to the add-in NIC in the PCI slot on the far right, plug power cords **into both jacks** and turn on power.
2. Director **default IP Address is 192.168.1.100**, subnet mask of 255.255.255.0.
3. **Connect to Director**, set your computer IP to 192.168.1.101 and **enter the URL** of Director in Address bar of IE (<https://192.168.1.100>) to display the Welcome Screen.
4. **Enter required network information** for each screen, then **Save and Reboot**.
5. While Director is rebooting, **reconfigure your computer to a live IP address** within the same network as the newly configured IP Address for the Director.
6. After reboot, **access Director from IE with the new IP Address**, to display the login screen.
7. After login, the **Setup Wizard** is displayed. Follow the step-by-step instructions to assign settings.
8. Click **Save** when complete. Settings are saved and the login screen is redisplayed.

### Note:

For detailed instructions of each step, refer to the remainder of this document.

# eTrust™ Vulnerability Manager Director



Computer Associates®

## eTrust Vulnerability Manager-Director Setup and Configuration

### Connect appliance to the network

1. Mount Director in a rack in accordance with the hardware vendor instructions.
2. At the back of Director, plug in a live network cable to the add-on **NIC in the PCI slot** on the far right side of the appliance.
3. Plug power into Director. There are 2 live power jacks and both must be used.
4. The default IP Address and Subnet Mask of Director will be pre-configured at:



IP Address – 192.168.1.100  
Subnet Mask – 255.255.255.0

5. Connect Director to a configuration machine.
  - a) If your network **uses the private network 192.168.1** and the address **192.168.1.100** is available, connect Director directly to that network and configure it from another browser-enabled computer (laptop or PC) on the 192.168.1 network.
  - b) If your network **does not use the 192.168.1 network**, or **uses the 192.168.1 network and the 192.168.1.100 address is already in use**, perform the initial configuration of Director from a machine connected to a temporary network. This temporary network can be a crossover cable, connecting Director to the configuration machine, or both machines connected to a hub/switch not connected to the rest of the network.

### To set up Director you will need:

1. Network and Internet connectivity and cables
2. A laptop, PC, or server with IE 5.0 or higher installed to access Director

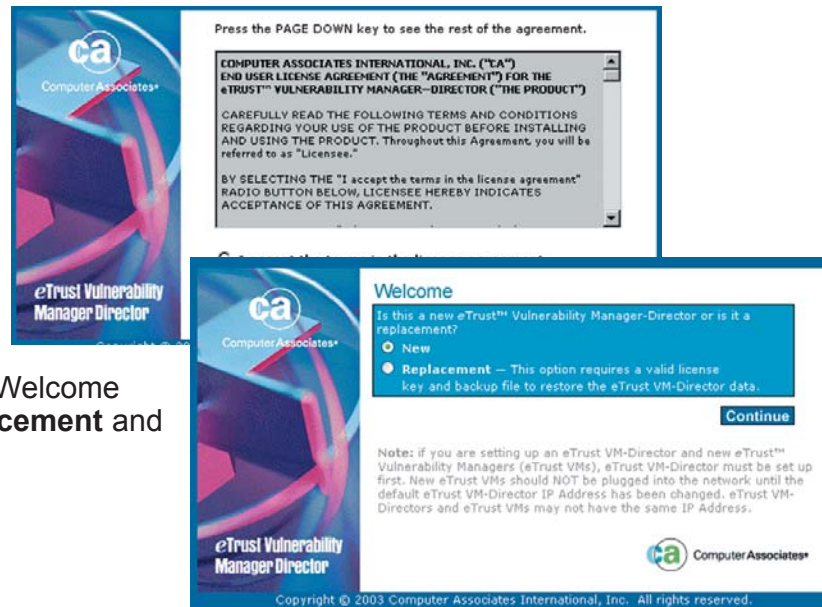
# eTrust™ Vulnerability Manager Director

6. After connecting Director to the configuration machine, turn on the power. The blue light circled on the picture at right indicates power is on. (This picture is the front of the Director with the bezel removed.)
7. Launch an Internet Browser (IE5.0 and higher or equivalent) from a computer connected to the same network as Director.
8. Enter the URL (<https://192.168.1.100>) of Director into the Address Bar. Upon initial connection, a Security Alert Certificate is displayed. Accept the certificate to continue. The License Agreement will be displayed.



## License Agreement Page

From the License Agreement page, scroll down to view the entire agreement. Accept the agreement and click **Continue**.



## Welcome Screen

After accepting the License Agreement, the Welcome Screen is displayed. Choose **New** or **Replacement** and click **Continue**.

The Network Information is displayed next.

### Note:

All Directors and eTrust VMs are shipped with same default IP address. To avoid IP conflict during Director set up, configure the Director before configuring any eTrust VMs into your network.

# eTrust™ Vulnerability Manager Director



Computer Associates®

## Login and Network Information

1. Create a **password** for the default administrator account.
  - a. Guidelines: 7-14 characters, case sensitive. Must contain 2 of the following: 1 upper case alpha, 1 lower case alpha, 1 special character, 1 numeric character.
2. **Define** the Director network **IP Addresses**.
  - a. Enter the Director Host Name.
  - b. Reconfigure the Director with an IP Address that resides within your network. This IP Address will be used later to access Director.
  - c. Enter the Subnet Mask, Default Gateway, and DNS Server IP Addresses associated with the Director IP Address.
3. If a **Proxy server** is used to access the Internet, enter the URL and the Port # and the login credentials, if required by the Proxy configuration. (ex. 10.10.10.10:80)
4. If your network uses a **time server**, enter the time server's IP address, or set the Director Clock to the current time. Click **Continue**.

### Note:

### Record Director Network Information

Password \_\_\_\_\_

Host Name \_\_\_\_\_

IP Address \_\_\_\_\_

Subnet Mask \_\_\_\_\_

Gateway \_\_\_\_\_

DNS Svr \_\_\_\_\_

Proxy URL \_\_\_\_\_

The screenshot shows the 'eTrust™ Vulnerability Manager-Director' configuration window. It is divided into several sections: 'LOGIN INSTRUCTIONS', 'NETWORK INSTRUCTIONS', 'PROXY INSTRUCTIONS', and 'DATE/TIME INSTRUCTIONS'. The 'Login' section has fields for 'Login Name' (set to 'administrator'), 'Password', and 'Confirm Password'. The 'Network' section has fields for 'eTrust VM-Director Host Name' (set to 'DIRECTOR'), 'eTrust VM-Director IP Address' (set to '111.11.111.11'), 'Subnet Mask' (set to '255.255.255.0'), 'Default Gateway' (set to '111.11.111.1'), and 'DNS Server' (set to '121.22.2.2'). The 'Proxy' section has fields for 'Proxy URL' (set to '125.25.250.25:80'), 'Login Name', and 'Password'. The 'Date/Time' section has fields for 'Time Server' (set to '125.25.250.25'), 'eTrust VM-Director Clock' (set to '9:22:00 AM'), and 'Adjust for Daylight Savings' (checked). The 'Current eTrust VM-Director Date/Time' is shown as '9/15/2003 9:22:08 AM'. There are 'Cancel' and 'Continue' buttons at the bottom right.

# eTrust™ Vulnerability Manager Director

## Route Table

The Route Table is an optional path allowing communication with Director via multiple paths. If it is not necessary to add a route, **Click Save and Reboot**.

To Add Network Routes:

1. Indicate the IP Address of the destination.
2. Indicate the Subnet Mask for that network.
3. Indicate the Gateway for that network.
4. Click **Add Route** and repeat steps as necessary.
5. Click **Delete** to remove a route.

When network settings are complete, click **Save and Reboot**. The reboot process can take up to eight minutes. After reboot, the Network settings will be applied to the Director.

The screenshot shows the 'ROUTE INFORMATION' window in the eTrust™ Vulnerability Manager-Director interface. It is divided into two main sections: 'ROUTE TABLE INSTRUCTIONS' and 'Route Table'. The instructions section contains a paragraph explaining the route table and a numbered list of steps: 1. Indicate the destination network or IP Address, 2. Indicate the Subnet Mask, 3. Indicate the Gateway, 4. Select the Add Route button and repeat steps as necessary, and a note to select Delete to remove a route. The 'Route Table' section has three rows of input fields for 'Destination Network', 'Subnet Mask', and 'Gateway', each with four boxes for digits. Below these fields is an 'Add Route' button. At the bottom of the window are 'Back', 'Cancel', and 'Save & Reboot' buttons.

The eTrust VM-D is rebooting. Please wait a few minutes then click [here](#).

## Completing the Configuration-Connect to the Director

1. While Director is rebooting, **reconfigure your machine** to an appropriate IP address within the network of the newly assigned IP address of Director.
2. After Director reboots, connect to it from a browser-enabled computer. If the machine has been continuously connected to the network, a page will display with a link to the new IP address saved in the Network Settings. Otherwise, **enter Director's new URL** (e.g. <https://10.1.1.100>) in the browser's address bar to finish configuration of Director.

### Note:

If one or more eTrust VMs and the Director are received at the same time, the Director *must* be configured first.

# eTrust™ Vulnerability Manager Director



Computer Associates®

3. Login to the Director with the user name “administrator” and the password created.
4. The Network Check screen will be displayed, indicating if the network information provided was ‘Passed’ or ‘Failed’. Click **Continue**.

If the check failed, the Network Information screen will redisplay. Reconfigure the Director.

If the check passed, the Setup Wizard will be displayed. Instructions continue on the next page.

5. For Replacement Directors: See the Restore section on the last page of this guide.

## Note:

If the network assigned to the Director does not require the use of a proxy for Internet connections, the firewall must be modified to allow the Director IP address access to the Internet through **port 443**.



## Troubleshooting

If an error is received when trying to access the Director URL, one of the following may have occurred:

- The Director has not completed the reboot; wait the full 8 minutes and retry.
- The "s" may have been left out of the URL; make sure https is manually typed (e.g. **https://1.1.1.1/**)
- Your workstation IP address has not been changed back to the same network as Director.
- The Director IP Address is invalid or not accessible from your network. Take the following action:
  1. Change the IP of your workstation to an IP within the network of the newly assigned Director IP.
  2. Isolate the network of the Director and the workstation by using a cross-over cable.
  3. Type the previously assigned IP address into a browser address bar.
  4. From the Management Tab > Network > page, reconfigure the IP Address.

# eTrust™ Vulnerability Manager Director

## Director Settings – Setup Wizard

The Setup Wizard offers a step-by-step guide to assist the user in completing the setup. Director settings are determined at this time.

### License Key

1. Enter the Director license key.
2. Click **Continue** to validate the license key and proceed with operational settings.

The screenshot shows the 'License Key' step of the Setup Wizard. The title bar reads 'eTrust™ Vulnerability Manager-Director'. The window title is 'SETUP WIZARD' with a note '\* Indicates required field.'. The main heading is 'License Key'. Below it, a message states: 'Enter the License Key. The License Key data will be sent to Computer Associates (CA) for validation. When the License Key is approved, you will be allowed to advance through the rest of the setup.' There is a single text input field labeled '\* License Key:'. A 'Continue' button is located at the bottom right.

### Content Updates and Purchased By Information

3. Select the **frequency** for updates to occur, daily or hourly. If daily, select the time of day.
4. Provide the **Purchased By** information for registration purposes. This information will be used solely for user support, content subscription and software maintenance renewal purposes.
5. (Optional) Provide Information identifying the Seller of this Director.
6. Click **Continue** to proceed.

The screenshot shows the 'Content and Purchaser Information' step of the Setup Wizard. The title bar reads 'eTrust™ Vulnerability Manager-Director'. The window title is 'SETUP WIZARD' with a note '\* Indicates required field.'. The main heading is 'Content and Purchaser Information'. Below it, the section 'Content Updates' asks to 'Select the frequency of the content updates.' with radio buttons for 'Hourly' (selected) and 'Daily'. A dropdown menu shows 'Midnight'. The 'Purchased By' section has fields for '\* Name:', '\* Telephone #:', and '\* Address:'. The 'Sold By' section has fields for 'Name:', 'Telephone #:', and 'Address:'. Both address fields include a note: 'Include street, city, state and zip code.' A 'Continue' button is at the bottom right.

### Note:

The Director must have internet connectivity in order to validate the license key and complete the setup.

# eTrust™ Vulnerability Manager Director



Computer Associates®

## Start Time For Maintenance and Backup Settings

Maintenance of the Director refers to code updates to the application and backup of data. See the **Maintenance** section of the User Guide, accessed from the Helpfiles, for complete details.

1. **Select the time of day** to initiate maintenance of the Director (the appliance will be inaccessible during the process).
2. **Select the appropriate backup settings**, Inactive, UNC format or FTP format.
3. Indicate the backup location and access information as appropriate, for the process selected.
  - a. Inactive: no entry required
  - b. UNC format (ex. \\192.168.1.100\backup\_drive) or FTP format (ex. ftp://192.168.1.100/backup\_drive)

*If using the server name instead of an IP Address, the entire domain name (FQDN) must be used (ex. file01.corp.com).*
4. Provide the username and password that allows write access to the backup location.
5. Click **Continue** to proceed.

### Note:

Maintenance for the Director should be scheduled for non-business hours if possible, as the Director will not be accessible during this time.

SETUP WIZARD \*Indicates required field.

**Start Time/Backup**

**Start Time for Maintenance**  
Maintenance of eTrust VM-D applies to application code updates and backup of all data.  
\* Start time:

**Backup Settings**  
Indicate a secure location to backup eTrust VM-D files.

**Inactive**  
NO backup will be performed.

**Active: Universal Naming Convention (UNC)**  
(ex. \\192.168.1.1\backup\_share)

**Active: File Transfer Protocol (FTP)**  
(ex. 192.168.1.1)

\* Path:   
Server must reside within eTrust VM-D's local network.

\* Username:   
\* Password:

# eTrust™ Vulnerability Manager Director

## Compliance Targets

Set the desired compliance levels for Vulnerabilities and Configuration Standards. This information is used for Compliance reports. The Director compliance targets have the following default settings:

- Vulnerabilities
  - High – 85%
  - Medium – 70%
  - Low – 50%
- Configuration Standards
  - High – 85%
  - Medium – 70%
  - Low – 50%

## Complete Director Setup

After completing all information in the setup wizard, click **Save** to complete the configuration. The login screen is displayed.

The screenshot shows the 'SETUP WIZARD' window for 'eTrust™ Vulnerability Manager-Director'. The 'Compliance Targets' section contains the following information:

The target values are used in the Compliance Reports for Vulnerabilities and Configuration Standards. Tasks that are compliant have a status of Implemented, Mitigate Risk, or Does Not Apply. Tasks with a status of Accept Risk are considered a risk exposure and are not in compliance. Targets represent your organization's compliance goals.

Compliance Target for Vulnerabilities (percent compliant):

- High:  %
- Medium:  %
- Low:  %

Compliance Target for Configuration Standards (percent compliant):

- High:  %
- Medium:  %
- Low:  %

**Completion of Setup**  
The setup wizard will be complete when you select the Save button.

Buttons: Back, Save

The screenshot shows the login screen for 'eTrust Vulnerability Manager Director'. It features the 'ca Computer Associates' logo on the left and a login form on the right. The login form includes the text 'Please login:' followed by 'User Name:' and 'Password:' labels, each with a corresponding text input field. An 'OK' button is located to the right of the password field. The 'eTrust Vulnerability Manager Director' logo and 'Computer Associates' logo are also present at the bottom of the screen. Copyright information at the bottom reads: 'Copyright © 2003 Computer Associates International, Inc. All rights reserved.'

### Note:

The eTrust Vulnerability Manager-Director User Guide, available in pdf version within the Helpfiles, provides complete instructions.

# eTrust™ Vulnerability Manager Director



Computer Associates®

## Restore

When installing a replacement Director, the user can upload a backup for a full restore. A restore can be performed on demand. When performing a system restore, users may select from the available back-up files, created by the previous Director, of the same version.

To restore data:

1. Define the method of the restore (based on the backup method).
2. Indicate the backup location and access information as appropriate.
3. Enter the username and password that allows read access to the backup location.
4. Click **Continue**.

For more information, see the Restore Data section of the eTrust VM Director User Guide.

## Questions

If you have questions about the installation, please refer to the Director User Guide, the Helpfiles, or contact Computer Associates at [www.esupport.ca.com](http://www.esupport.ca.com).



