eTrust™ Vulnerability Manager-Director

User Guide
Version 1.0

Computer Associates™

TABLE OF CONTENTS

INTRODUCTION

The *e*Trust™ VM-Director from Computer Associates International, Inc. (CA) allows organizations to manage enterprise security by strategically distributing multiple *e*Trust Vulnerability Managers throughout a network. It provides a scalable vulnerability management solution for complex enterprise networks. Using the eTrust VM-Director, administrators can easily manage multiple *e*Trust Vulnerability Managers. In addition, it offers executive management a centralized management console for an accurate picture of the enterprise security posture.

*e*Trust™ Vulnerability Manager is an asset-based solution that simplifies vulnerability management by discovering critical assets and the technologies running on them, correlating them with validated vulnerabilities and providing risk-based task lists with step-by-step remediation instructions. *e*Trust VM includes a comprehensive vulnerability database and web-based access — helping to proactively protect your organization before your systems are compromised.

FUNCTIONALITY OVERVIEW

REPORTING

Compliance and Performance reports for vulnerabilities and configuration standards are available from the eTrust VM-Director. Reports will apply to one eTrust VM, multiple eTrust VMs or a specified group of eTrust VMs.

ACCOUNT ADMINISTRATION

Administrators have access to all User functions, as well as additional administrative functions, including the ability to create and edit user accounts for the eTrust VM-Director.

CODE AND CONTENT UPDATE

Content and code update requests will be issued on either an hourly or daily basis. Content and code updates are always initiated/requested by the eTrust VM-Director; CA will never "push" these updates to the eTrust VM-Director. The system will initiate a single request for all content types and update this content for all eTrust VMs managed by the eTrust VM-Director.

SYSTEM BACK-UP AND RESTORES

During the set-up process, the administrator can elect to activate the daily back-up process, and define the start time for the maintenance window. System restores can be performed on demand.

ACCESS CONTROL

The eTrust VM-Director will support two types of users – the Administrator and the User. The User will have access to all reporting and view the status of eTrust VMs being managed. The Administrator will have access to all User functions in addition to the administration functions as defined in this document.

Communication between a user and the eTrust VM-Director is accomplished using anonymous SSL. A login process consisting of a user name and password combination is used to authenticate the user. In order for the unit to receive updates, a unique identifier, the License Key, is used to verify that the requesting unit is a valid and active eTrust VM-Director. Security patches are contained in maintenance code releases and are fully tested during the CA QA process.

MANAGEMENT

The eTrust VM-Director can support the management of up to 25 eTrust VMs, and can support a maximum of 200 users. By setting an eTrust VM's Content Source to eTrust VM-Director, along with that IP address, the eTrust VM becomes a 'managed device' for that eTrust VM-Director. The eTrust VM-Director will verify that the license will allow the addition of the eTrust VM and validate the eTrust VM License Key information prior to transmitting update data.

SETUP AND CONFIGURATION

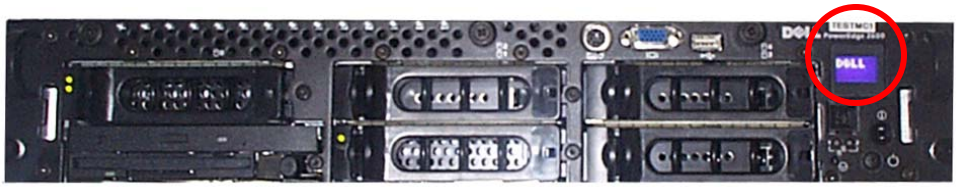
CONNECT *e*TRUST VM-DIRECTOR TO THE NETWORK

1. Mount eTrust VM-Director on a rack in accordance with the hardware vendor instructions.
2. At the back of eTrust VM-Director, plug in a live network cable to the add-on **NIC "2**" on the right side of the eTrust VM-Director.
3. Plug power into the two live jacks (both must be used).

4. The default IP Address and Subnet Mask of eTrust VM-Director is pre-configured at:
   IP Address – 192.168.1.100
   Subnet Mask – 255.255.255.0

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

6. After connecting eTrust VM-Director to the configuration machine, turn on the power to boot up. A blue light will be lit, indicating power is on. (The picture below is the front of the eTrust VM-Director with the bezel removed.)

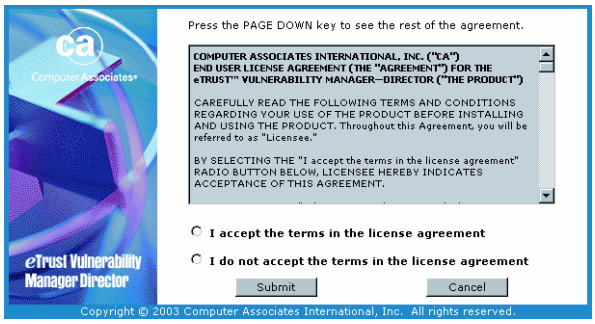


7. Launch an Internet Browser (IE5.0 and higher or equivalent) from a computer connected to the same network as eTrust VM-Director.
8. Enter the URL (IP Address) of eTrust VM-Director into the Address Bar (https://192.168.1.100) to complete the configuration.

LICENSE AGREEMENT PAGE

After accessing the eTrust VM-Director URL(https://192.168.1.100) and accepting the Security Alert Certificate, the License Agreement screen is displayed.
From this page:

1. Scroll down to read the entire License Agreement.
2. Click the radio button to **Accept** the agreement.
3. Click **Submit**.

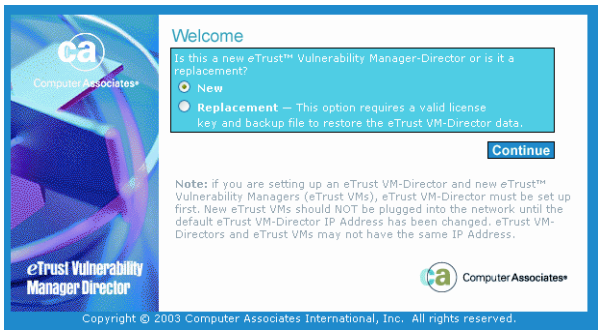


WELCOME SCREEN

After accepting the License Agreement, the Welcome Screen is displayed.

1. Select **New** Configuration of this appliance or **Replacement** configuration of a previous management console.
2. Click **Continue**.

If **New** is selected, the network information is displayed.
If **Replacement** is selected, the Restore Screen displayed.

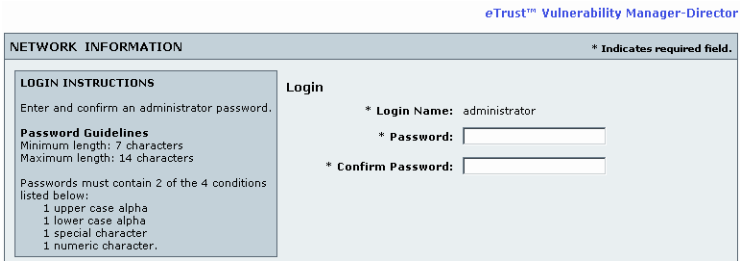


NETWORK INFORMATION

Login Name and Password

eTrust VM-Director is delivered with a default Administrator account, which is displayed in the Login Name field.

1. Select a password for the default administrator login name.
2. Retype the password to confirm it. ***Be sure to record this password for use after the initial setup***



Guidelines for Setting Passwords

Select a Password that meets the following criteria:

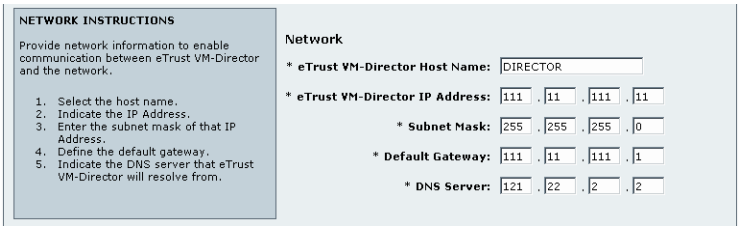
Passwords are case sensitive
Minimum length - 7 characters
Maximum length - 14 characters
Passwords must contain 2 of the 4 conditions listed below:
1 upper case letter
1 lower case letter
1 special character (*,#,!,$, etc)
1 number

- Passwords will not expire and no password history will be kept.
- Administrators will be able to change user account passwords.
- If a User fails to provide the correct password after 5 attempts, the account will be locked.
- The User account can be unlocked by an Administrator or the application will unlock the account after 24 hours has elapsed from the time the account became locked.
- Administrator accounts will be unlocked when eTrust VM-Director is re-booted.
- The session timeout is set to 60 minutes.

Network Addresses

The Network Information fields are used to further define the network settings of eTrust VM-Director.

- Select the **Host Name**.
- Define the **eTrust VM-Director IP Address.**
- Indicate the **Subnet Mask** of that IP Address.
- Define the **Default Gateway**.
- Indicate the **DNS server** eTrust VM-Director will resolve from.



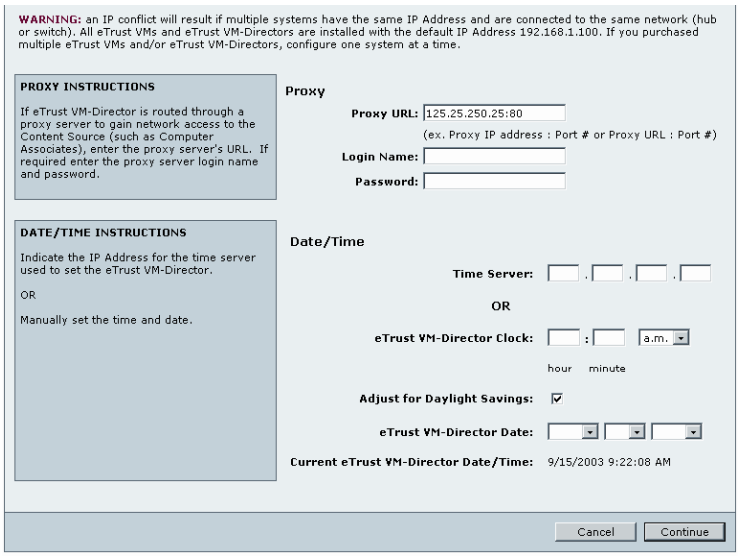
If unsure of the IP Addresses of any of the above fields, contact your Network Administrator. ***Be sure to record all IP Addresses entered on this screen for future reference.***

WARNING: For multiple eTrust VM-Director setups, configure one eTrust VM-Director before plugging the next into your network. Because the eTrust VM-Directors are all shipped with the same default IP address, problems will occur if not performed in this sequence.

Proxy Settings

In the Proxy URL field, indicate the URL and/or IP Address of the Proxy Server. Based on the configuration of that Proxy, the port number, login name and/or password may also be required to obtain access.

- The **URL or IP Address** is mandatory.
- The **Port #** must be included in the Proxy URL field, if required by the configuration of that Proxy.
  Examples: **100.100.12.120:80**
  corp.com:80
- The **login name and password** are not mandatory, unless required by the configuration of that Proxy.



Date/Time Settings

In the **Time Server** field:
Indicate the IP Address of the time server used to set the eTrust VM-Director clock….or……If a timeserver is not used, the clock must be manually set.

In the **eTrust VM-Director Clock and Date** fields:

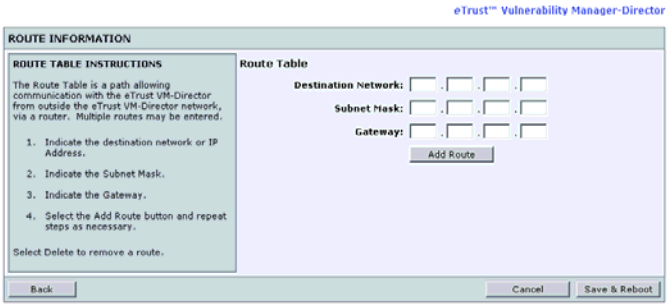
1. Manually set eTrust VM-Director time and date.
2. Indicate if Daylight Savings Time should be observed.
3. Click **Continue**.

Route Table

The Route Table is an optional path allowing communication with eTrust VM-Director via multiple paths.

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.

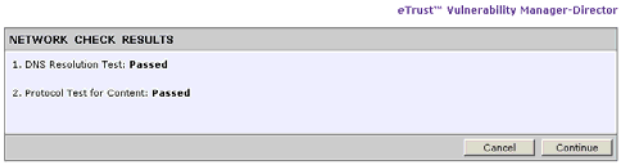


When network settings are complete, click **Save and Reboot**. The Network settings will be applied to eTrust VM-Director.

COMPLETING THE CONFIGURATION

1. Change the workstation to an IP Address that is within the newly configured eTrust VM-Director Network.
2. It should take approximately 8 minutes to reboot.
3. After reboot, connect to it from a browser-enabled computer. If the machine has been continuously connected to the network, the reboot screen shown in the previous section will provide a link to the new IP address saved in the Network Settings. Otherwise, enter the new URL (e.g. https://10.1.1.100) in the browser's address bar to finish configuration of eTrust VM-Director. The login screen is displayed.

4. After login, 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 eTrust VM-Directors: After the login process, the **Restore** process will automatically initiate. Instructions continue with the Restore section below.

TROUBLESHOOTING TIPS

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

- The eTrust VM-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 the **https** is manually entered (e.g. https://1.1.1.1/)
- Your workstation IP address has not been changed back to the same network as eTrust VM-Director. Test this by pinging the new IP Address from your workstation.
- The eTrust VM-Director IP Address is invalid or not accessible from your network. If this happens, take the following action:

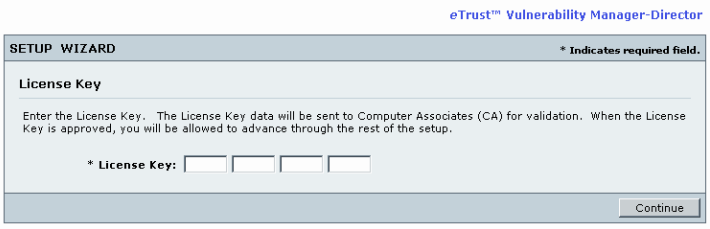
1. Change the IP Address of your workstation to an IP within the network of the newly assigned eTrust VM-Directors IP.
2. Isolate the network of the eTrust VM-Director and the workstation by using a cross-over cable.
3. Type the previously assigned IP address into a browser address bar.
4. From the Management Tab > Network page, reconfigure the IP Address.

SETUP WIZARD

The Setup Wizard offers a step-by-step guide to assist the user in completing the setup. eTrust VM-Director settings are determined at this time, but can be changed later through the Management Tab. After the system reboots and the administrator logs in, the setup wizard will be displayed to provide an organized, sequential navigation to the pages required for setting up eTrust VM-Director functionality. Steps in the wizard include:

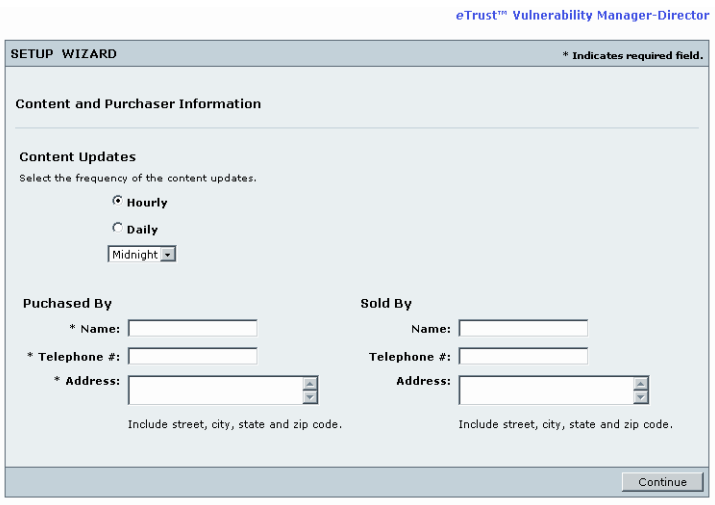
- License Key and Terms and Conditions
- Content Information
- Maintenance and Backup Settings
- Compliance Targets

ENTER LICENSE KEY



During Step 1 of the setup, the eTrust VM-Director license key is entered. The License Key will be validated at time of setup, at the end of the Setup wizard. After validation, this information cannot be modified. Only when the license key has been validated will eTrust VMs be allowed to "register" with the eTrust VM-Director.

CONTENT UPDATES



Step 2 of the eTrust VM-Director setup process defines the interval that content updates will be delivered: hourly or daily. Those settings indicate a time to initiate communication to CA to send the updates. At that time, the content is downloaded to a holding area, awaiting the scheduled maintenance, which is indicated in the next step. See the Content Updates section of the Management Tab for more details.

1. Select **Hourly** or **Daily**.
2. If Daily is selected, **indicate the hour of the day** for eTrust VM-Director to request updates.

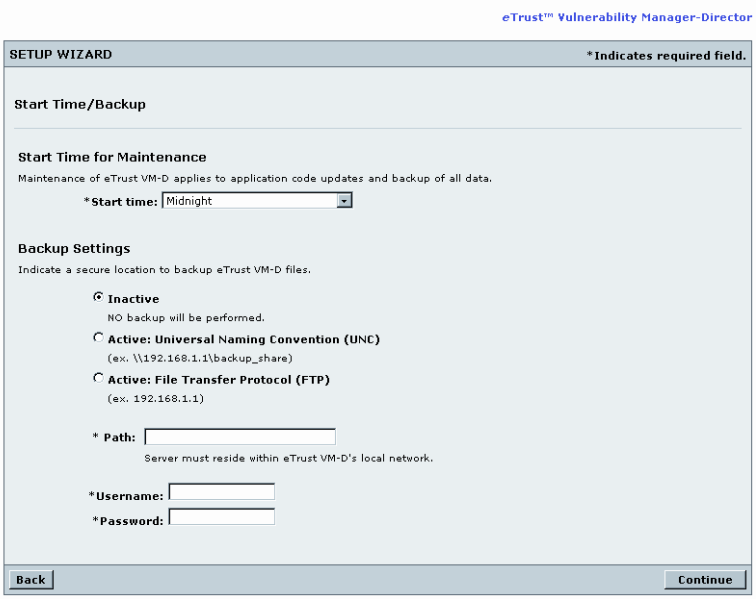
PURCHASED AND SOLD BY INFORMATION

The **Purchased By** (mandatory) and **Sold By** (optional) information should be added, including the name, telephone number and address for each. Click **Continue** to validate the License Key and continue to the eTrust VM-Director Settings.

START TIME FOR MAINTENANCE

Step 3 of the eTrust VM-Director setup defines the start time in which maintenance for the eTrust VM-Director will occur, backup settings and backup credentials. Content updates were previously scheduled on the last screen. Those settings indicated a time to initiate communication to CA to send the updates. At that time, the content is downloaded to a holding area, awaiting the scheduled maintenance, which is indicated in this step. See the Maintenance section for more details.

1. Indicate the **start time** for Maintenance of eTrust VM-Director.
2. eTrust VM-Director will be down during the maintenance process. Schedule updates for non-business hours.



BACKUP SETTINGS

During the set-up process, the user can elect to activate the automated daily Backup of files.

If backup settings **ARE** enabled, the eTrust VM-Director database files will be backed up as part of the maintenance process, according to the scheduled time and location, an FTP or UNC location. Each backup will be a separate file with a new name.

If this option is **NOT** enabled, back up will not occur. See the Maintenance section for more details.

Indicate the location and access information to place the backup files. Ensure these access control devices have the appropriate ports open to the eTrust VM-Director IP.

1. Select **ONE** of the following radio buttons.
   a) **Inactive** –No backup will be performed
   b) **Active Universal Naming Convention (UNC)**
   c) **Active File Transfer Protocol (FTP)**

2. If an Active UNC or FTP is indicated, define the **Path**.
   a) **UNC** (ex. \\192.168.1.100\backup_share)
   b) **FTP** (ex. ftp://192.168.1.100/backup_drive)
      Note: If using the server name instead of an IP Address, the entire domain name (FQDN) must be used (ex. **File01.corp.com**).

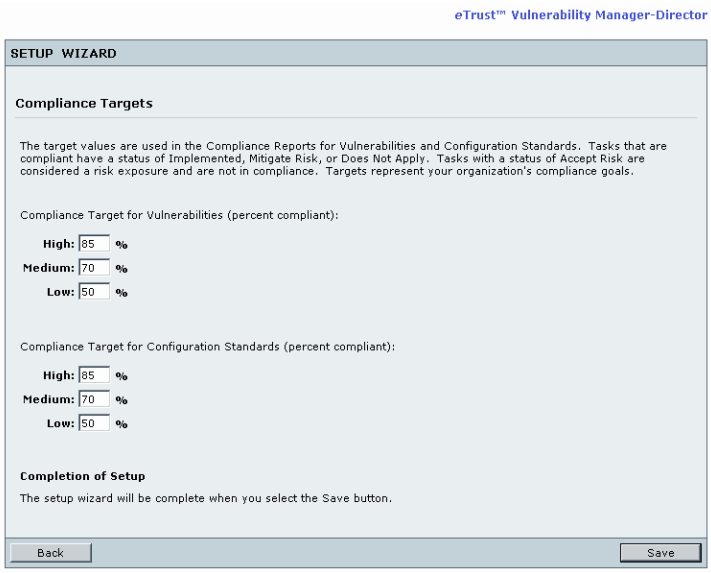
3. Enter the **username and password** that allows access to the backup location.
4. Click **Continue** to proceed.

COMPLIANCE TARGETS

Step 4 of the eTrust VM-Director setup defines the desired compliance levels for both Vulnerability and Configuration Standards. This information will be used for Compliance and Performance reports. The eTrust VM-Director compliance targets have the following default settings:

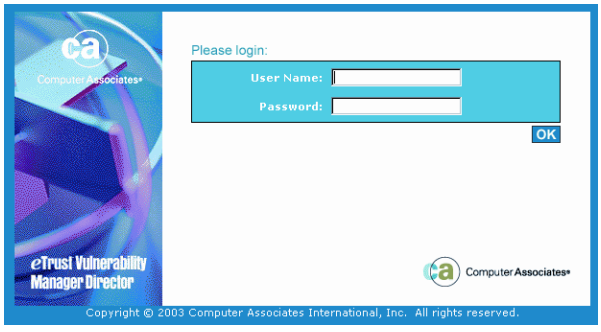
- Vulnerabilities
  - High – 85%
  - Medium – 70%
  - Low – 50%
- Configuration Standards
  - High – 85%
  - Medium – 70%
  - Low – 50 %

Change the percentages by typing numbers in the selected fields.



COMPLETE THE SETUP

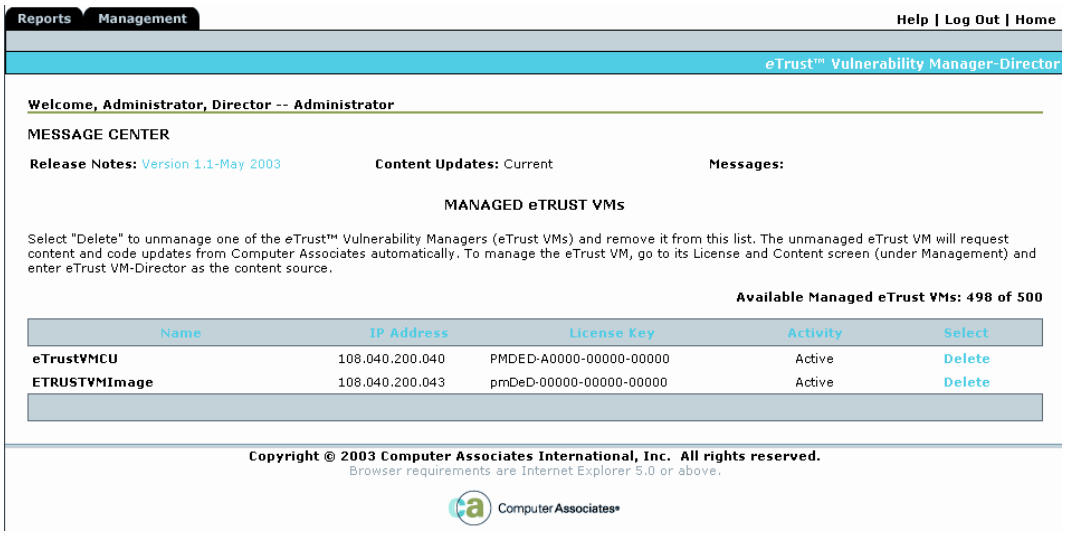
After completing all information in this setup wizard, click **Save**. If setup is accomplished, the login screen will be displayed.



HOME PAGE

Upon login, the home page will be displayed as shown below. Content within the home page includes:

1. Two Tab Navigation:
   - Reports
   - Management
2. The User name and eTrust VM-Director role at the top of the page
3. The Message Center, with links to:
   - Release Notes
   - Content Updates: Status
4. List of Managed eTrust VMs
5. Indicator for Current number of eTrust VMs managed vs. total number allowed
6. Links to access HelpFiles, to Logout, and to come back to this home page, available on all pages



RELEASE NOTES

Release Notes will be available to users via a link on the home page whenever a code update has been successfully implemented on a eTrust VM-Director. Major releases include new functionality or significant enhancements to existing functionality. Minor releases include fixes or patches.

CONTENT UPDATES

The Content Updates field on the home page displays the status of the update process. The Status message will provide an indication of the status of communication between CA and the eTrust VM-Director. Statuses include:

- **Current** – used to indicate content/code updates have been applied successfully.
- **Failed** – Contact Support" – upon the 5th consecutive transmission failure, this status will be displayed.
- **Code Update Pending** – used to indicate that a code update will be applied at the next start time of the maintenance window.
- **License Expired – Contact Support** – used to indicate that the last request for content/code from CA was denied because the eTrust VM-Director license was expired.

LIST OF MANAGED *e*TRUST VMS

The home page of eTrust VM-Director displays a list of eTrust VMs that are currently managed by this eTrust VM-Director. These eTrust VMs have registered with and have the content/code updates managed by the eTrust VM-Director. Both the User and Administrator roles will have access to this information. Information in the list of eTrust VMs includes:

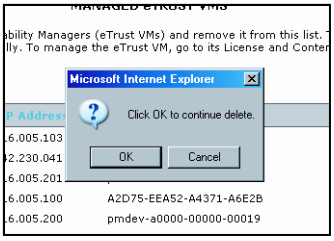
- The host **name** of each managed eTrust VM (if one was indicated in the eTrust VM setup).
- The **IP Address** of each managed eTrust VM.
- The **License Key** of each managed eTrust VM.
- The **Activity status** of each managed eTrust VM. Statuses are:
  - **Active** – indicates eTrust VM-Director and eTrust VM have been in communication in the last 24 hours.
  - **Inactive** – indicates eTrust VM has been unavailable for over 24 hours.
  - **Off-line** – indicates there has been no communication with the eTrust VM for more than seven days.
- A **delete link** available to the Administrator role only, to remove the eTrust VM from being managed by the eTrust VM-Director.
- The header will display the **current number of eTrust VMs managed** vs. the total number allowed. The maximum number of eTrust VMs that any one eTrust VM-Director is capable of managing is 25.

REGISTER AN *e*TRUST VM WITH THE *e*TRUST VM-DIRECTOR

When an eTrust VM makes the request to be added as Managed, it is registered with the eTrust VM-Director. This request is done by selecting eTrust VM-Director as the content source, during eTrust VM setup. The eTrust VM-Director will verify that its license will allow the addition of the eTrust VM. If the eTrust VM-Director's license will not allow an additional appliance License Key, an error message is sent to the eTrust VM. The eTrust VM-Director will validate the information prior to transmitting update data to the appliance.

DISASSOCIATE AN *e*TRUST VM FROM THE *e*TRUST VM-DIRECTOR

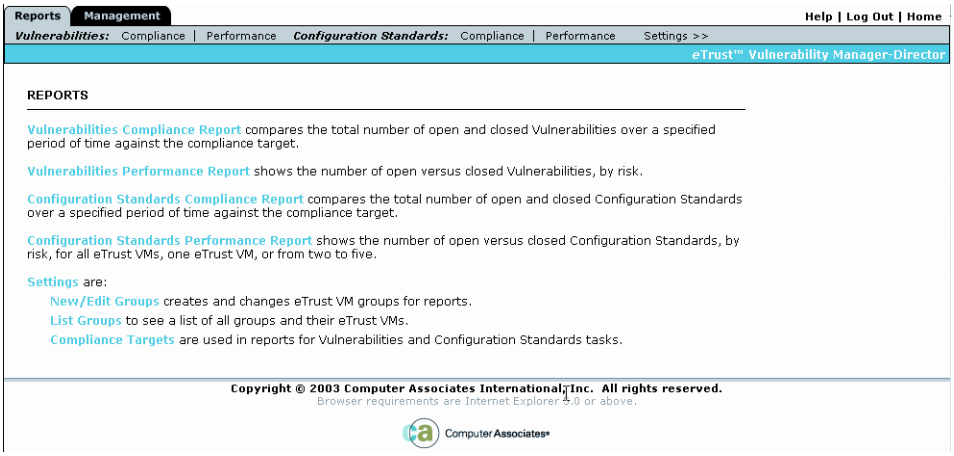
The administrator may remove an eTrust VM from the pool of eTrust VMs managed by the eTrust VM-Director by selecting the **delete** link. All associated data will be purged from the eTrust VM-Director for that **now** unmanaged eTrust VM. The system will display a message asking the user to confirm the suspension of management before executing the command. **At the time of deletion, the content source field in that eTrust VM will be automatically switched to CA**. At that point, the eTrust VM will no longer receive content or code updates from the eTrust VM-Director.



If the source of content for an eTrust VM is changed back to eTrust VM-Director, the eTrust VM will resend all data to the eTrust VM-Director. The system will display a message asking the user to confirm the addition of eTrust VM.

REPORTING

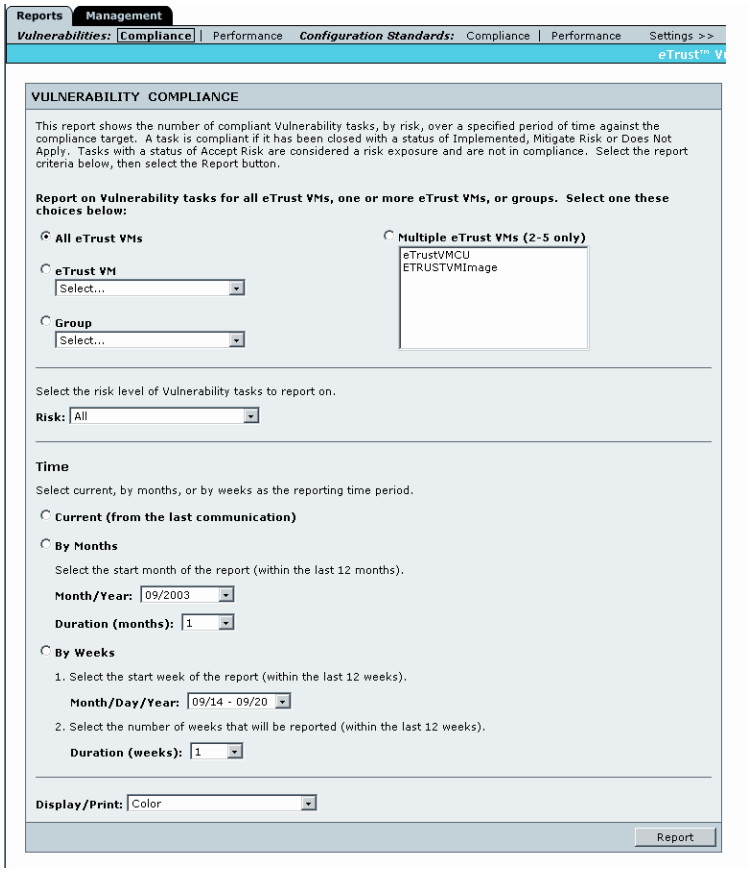
Management Reporting consists of two different types of reports: Compliance & Performance, and each report has a printer friendly option. These reports may be generated to provide a summary of a single eTrust VM, all managed eTrust VMs, a defined group of eTrust VM or multiple (2-5) eTrust VMs. Reports are presented in chart format and reflect a user-selected time period.



COMPLIANCE AND PERFORMANCE REPORTING

Compliance reports will provide an indication as to what extent individual appliance(s) or a selected group of eTrust VMs are meeting the compliance targets defined in the Settings. Compliance targets are defined as the percentage of closed Vulnerability or Configuration Standard tasks.

Performance reports will provide an indication as to how well individual eTrust VM(s) or a selected group of eTrust VMs are managing risk. Performance is defined as the number of open vs. closed vulnerabilities (and/or configuration standards) and can be evaluated at a point in time or over time.



REPORT OPTIONS

The following options are available for both Compliance and Performance reports:

- **Select eTrust VM(s)** to report on. Options are:
  1. **All** – If this option is selected, the data will be summarized across all managed eTrust VMs.
  2. **One eTrust VM** – A drop down list will display all managed eTrust VMs for this eTrust VM-Director and only one may be selected.
  3. **Group** – If this option is selected, the data will be summarized across all eTrust VMs associated with the eTrust VM Group selected.
  4. **Multiple eTrust VMs** (from two to five) – Data for each individual eTrust VM is shown on the report.
- **Select Risk** (only one option may be selected):
  1. **High, Medium or Low** – The data will be summarized by the risk selected.
  2. **All** – The data will show each risk category on the same graph except as noted in the *All* bullet.
- **Time Increments**
  1. **Current** –Data reported is for the "current" date (may be "current" as of midnight of the current day).
  2. **By Months** – The data will be collected continuously and month-end data stored for the most recent 12 months. The user can identify the number of months to be reported (max. 4) and the start month of the report.
  3. **By Weeks** – The data is collected continuously and end of week data stored for the most recent 12 weeks. User identifies the number of weeks to be reported (max. 4) and the start week of the report.

REPORT DATA RETURNED

- **Closed Task** = A task that has a status of: Accept Risk; Does Not Apply, Implemented, or Mitigate Risk.
- **Compliance Reports**
  1. **Compliance Target** – Set globally, this is defined as a target percentage closure rate by content type and risk.
  2. **Percentage of Compliant Tasks** – Displays the total number of Closed Tasks and total number of Open Tasks , for those tasks considered **Compliant** (status of Implemented, Mitigated and Does Not Apply)
- **Performance Reports**
  1. **Total Open Tasks** – Total number of open tasks within the selected risk level.
  2. **Total Closed Tasks** – Total number of closed tasks within the selected risk level.
- **Dates**
  1. **Current** – Data reflects the "state" at the indicated point in time.
  2. **Monthly** –Dates are month-end dates of selected time increments.
  3. **Weekly** –Dates are end of week dates of selected time increments. A week is defined as Sunday through Saturday.

Example reports are shown on the next page.

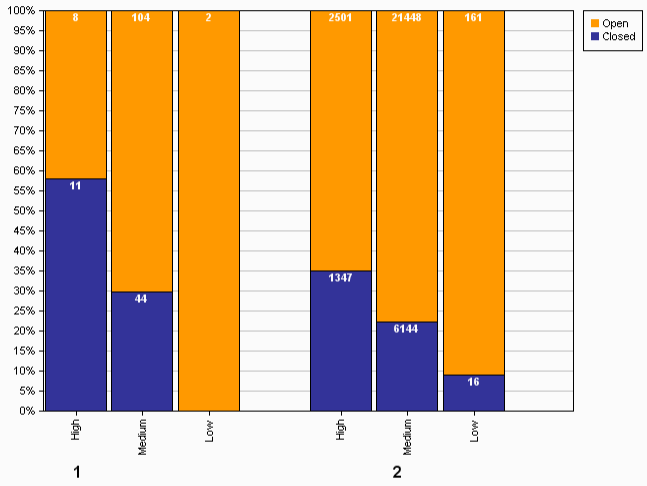
eTrust™ Vulnerability Manager

VULNERABILITY PERFORMANCE BY RISK REPORT

To print this report, select File > Print.

Report Date: 7/30/2003 1:19:20 PM

Vuln. Performance by Risk as of 7/30/2003



1. USILSS12

Total Vuln. 169 Assets 3

2. USILSS13

Total Vuln. 31,617 Assets 241

Selected eTrust VMs: USILSS12, USILSS13

eTrust VMs that have not communicated in the last 7 days: None

This report is all eTrust VM activity to date, including eTrust VMs that r

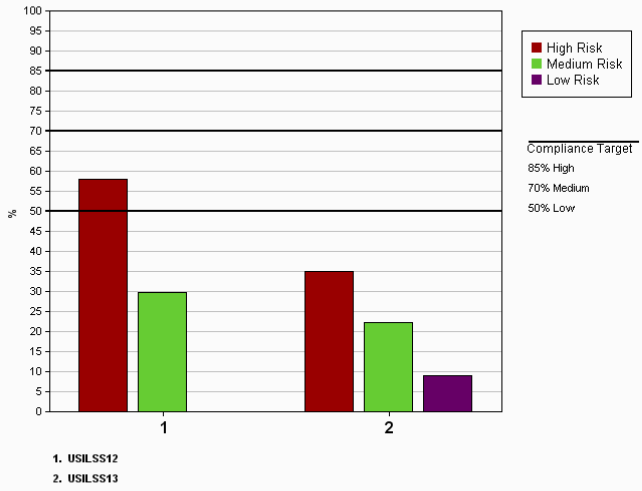
eTrust™ Vulnerability Manager

VULNERABILITY COMPLIANCE BY RISK REPORT

To print this report, select File > Print.

Report Date: 7/30/2003 1:19:20 PM

Vuln Compliance by Risk as of 7/30/2003



1. USILSS12

2. USILSS13

Selected eTrust VMs: USILSS12, USILSS13

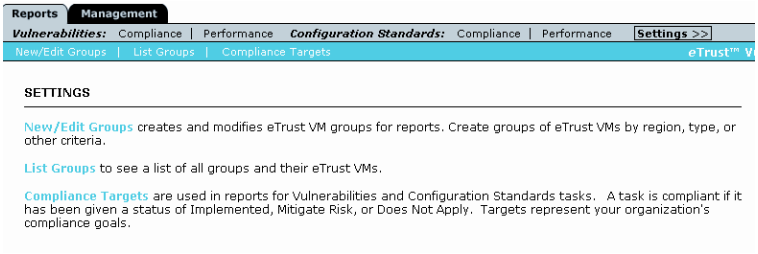
eTrust VMs that have not communicated in the last 7 days: None

This report is all eTrust VM activity to date, including eTrust VMs that may no longer be in contact with this eTrust VM-Director.

Computer Associates

GROUP SETTINGS

eTrust VM Groups can be created as a mechanism to roll-up data for the Performance and Compliance reports. The Administrator will have access to create, edit or delete an eTrust VM Group.



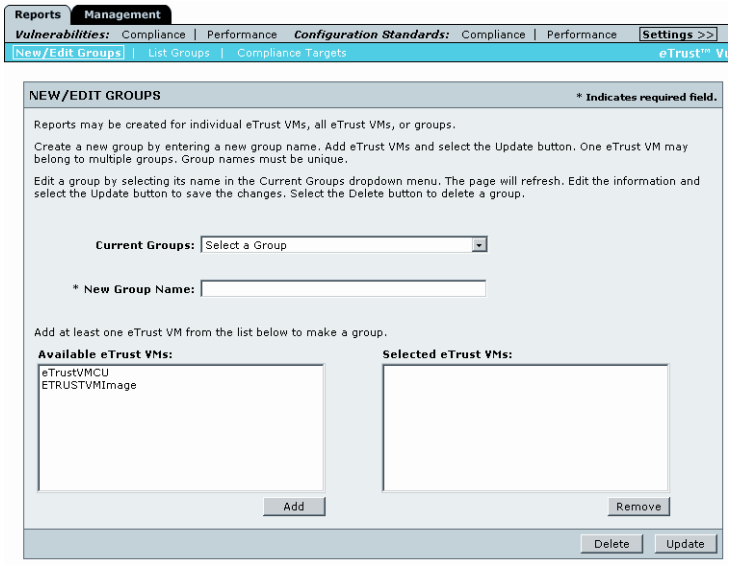
NEW/EDIT GROUPS

The Administrator may create, edit or delete an eTrust VM Group. The following rules apply:

- The eTrust VM Group Name must be unique and is a required field.
- The eTrust VM group will consist of 25 or less eTrust VMs that are being managed by the eTrust VM-Director.
- An eTrust VM can belong to multiple eTrust VM Groups.
- At least one eTrust VM must be selected in order to create or update a group.

To Create a New Group:

1. Type the **Group Name** if the field provided.
2. Click the **eTrust VM to add** to that group.
3. Click the **Add** button.
4. Repeat as necessary.
5. Click **Update** to save the new group.



To Edit a Group:

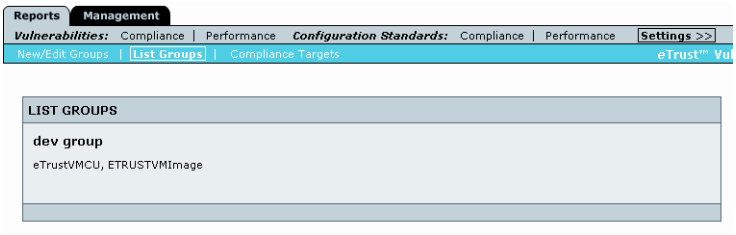
1. **Select the Group Name** from the dropdown menu of Current Groups.
2. Click the **eTrust VM to Add or Remove**.
3. Click the **Add or Remove** button.
4. Repeat as necessary.
5. Click **Update** to save the changes.

To Delete a Group:

1. **Select the Group Name** from the dropdown menu of Current Groups.
2. Click **Delete**.
3. Click **Update** to save the deletion.

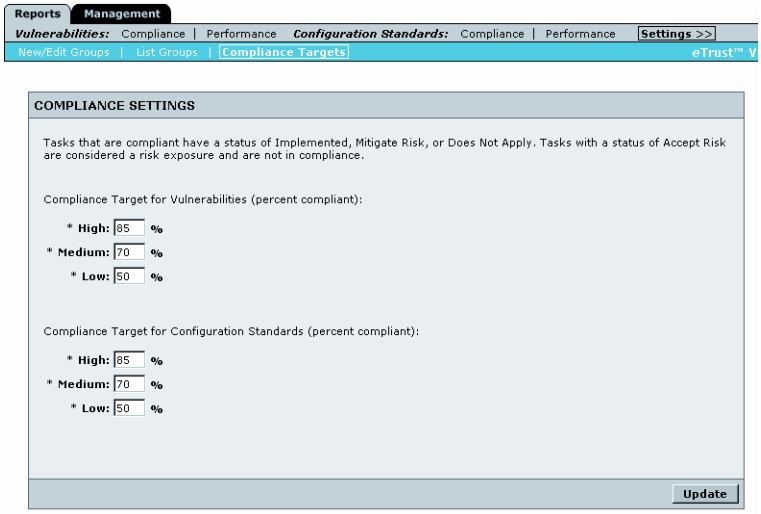
LIST GROUPS

The List Groups option displays a list of all eTrust VM Groups, along with all eTrust VMs that are associated with that group. No actions can be taken from this screen. Click the New/Edit Groups link to modify, add or delete groups.



COMPLIANCE TARGETS

The compliance targets are applied globally to all appliances that are managed by the eTrust VM-Director. The target value is captured and displayed as a percentage completion of vulnerabilities or configuration standards based on risk level.



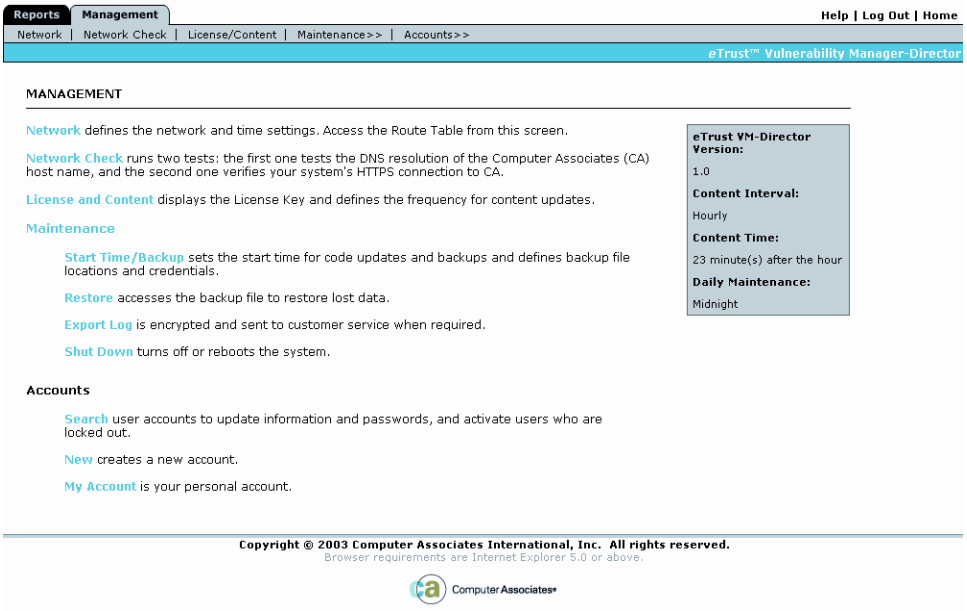
The default compliance targets are displayed in the eTrust VM-Director Setup and Configuration section. The values can be modified in the setup process as well as on the Reports > Settings > Compliance Targets page.

The values are displayed as a percentage (70%) and will be entered in the same manner (i.e., if the user enters 70, the result will be 70%; if the user enters 0.7, the result is 0.7 % or 0.007).

MANAGEMENT OF *e*TRUST VM-DIRECTOR

The Management tab is available to allow modification to eTrust VM-Director settings that were configured in the initial setup process. The overview page displays link to the various settings, as well as a eTrust VM-Director status box.

- **Network -** Defines network IP address, proxy settings, route tables and time settings of the eTrust VM-Director.
- **Network Check -** Administrator role only, runs tests to verify connections for Content Source and communication are set up properly.
- **License and Content** - Displays the license key and the content update schedule.
- **Maintenance**-Includes settings for start time, restore of data, troubleshooting and shutdown.
- **Accounts**-Displays user lists, create new accounts {admin only}, modify personal accounts.



MAINTENANCE STATUS

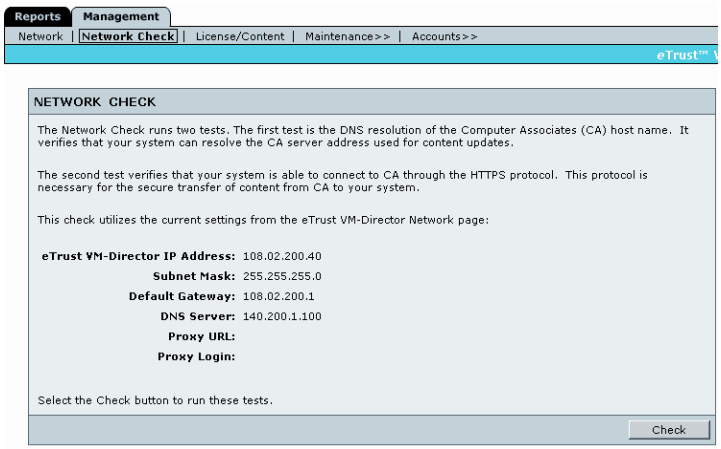
Also displayed on this page is a status box. The status box contains:

- **eTrust VM-Director Version**. This is the version of the current eTrust VM-Director release.
- **Content Interval.** This is determined from the License/Content page settings and will be either Daily or Hourly.
- **Content Time.** This is the time that the eTrust VM actually makes the request for content (in the instance above, that time is exactly on the hour). Other options would be: 5 minutes after the hour, 15 minutes after the hour, etc.
- **Daily Maintenance**. This is the scheduled time determined from the Start Time/Backup page settings (midnight in the instance above). The content is loaded to the holding area at the time specified (hourly in the instance above) and then the content and code is actually applied to the eTrust VM-Director at the scheduled Daily Maintenance time. See the Start Time Maintenance section for more information.

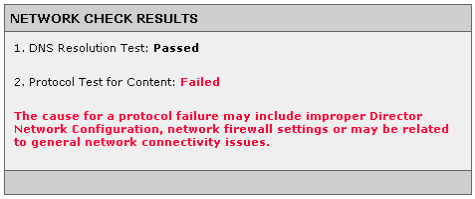
NETWORK CHECK

The Network Check function is available to the administrator role only. This check runs two tests.

1. The first test is the DNS resolution of the CA host name. It verifies that your system can resolve a CA server address.
2. The second test verifies that your system is able to connect to CA through the HTTPS Protocol. This protocol is necessary for the transfer of content from CA to your system. This check utilizes the current settings from the eTrust VM-Director Network page (the values will be listed).



The **Check** button at the bottom of the page executes the network checks. In the instance below, the **HTTP test failed**.



The message displayed for a **DNS Failed** result is:

The configured DNS for the eTrust VM-Director is unable to resolve the appropriate CA address. The cause for DNS failure may be related to eTrust VM-Director DNS configuration or to your configured DNS server.

NETWORK INFORMATION

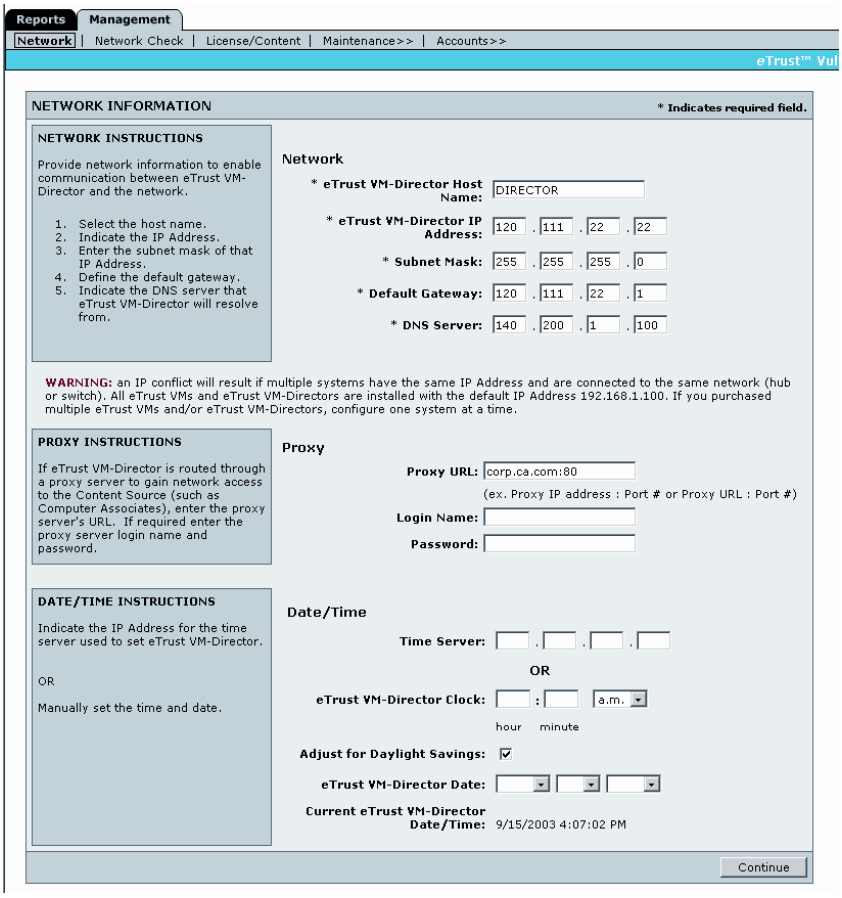
Network information for eTrust VM-Director was obtained at the initial setup. This information can be modified from the Management tab, but is not recommended. If IP Addresses are changed, each associated eTrust VM network information would need to be modified. See the Network Information section of Setup and Configuration, at the beginning of this User Guide, for complete instructions.

Proxy settings

See the Proxy Settings section of Setup and Configuration, at the beginning of this User Guide, for complete instructions.

Date/Time Settings

See the Date/Time Settings section of Setup and Configuration, at the beginning of this User Guide, for complete instructions.

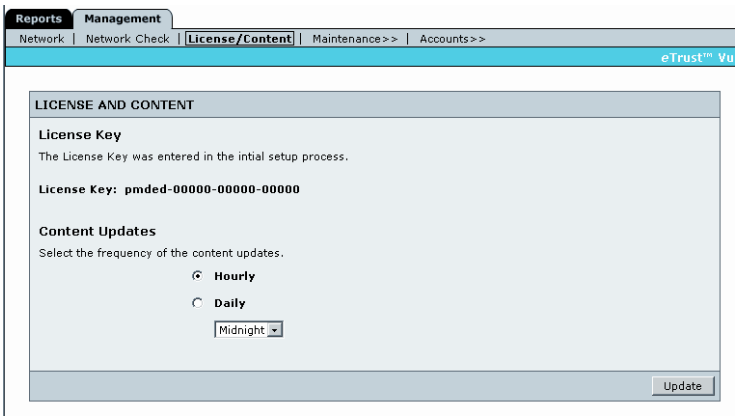


LICENSE AND CONTENT

The **License Key** field, displayed from the Management tab, allows the user to view the License Key for this eTrust VM-Director. The License Key was obtained in the setup process and cannot be modified. See the License Key section in the configuration process for more information. If a replacement unit is issued, the same license key will be used.

Content updates scheduled during the set up wizard can later be modified by an Administrator from the Management tab, License/Content link. These settings indicate a time to initiate communication to CA to send the updates. At that time, the content is downloaded to a holding area. The new content is added, but any code updates are held until the scheduled maintenance start time. The Maintenance Settings determine what time the code updates (sitting in the holding area) will actually be applied to each managed eTrust VM for this eTrust VM-Director. It is important to remember, when scheduling, that the eTrust VMs will be down at the time the code is applied.

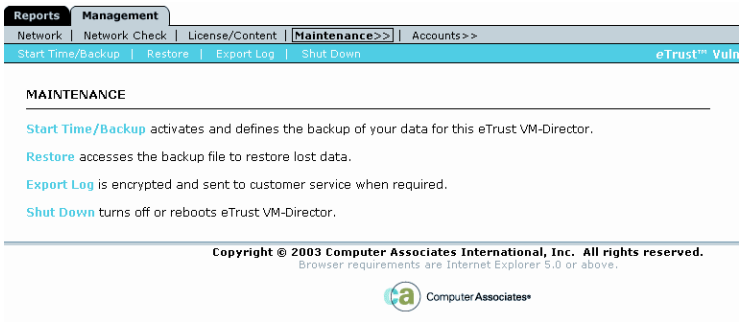
An Administrator can change the frequency and time that the eTrust VM-Director retrieves code and content updates from the CA. Frequency choices are hourly (default) or on a daily basis. If updates are selected on a daily basis, the time that the content will be pulled must also be selected.



MAINTENANCE

Maintenance of eTrust VM-Director applies to code updates to the application and backup of data. Maintenance and enhancements will be delivered to the eTrust VM-Director via the Content/Code Update process. The eTrust VM-Director will automatically apply updates with no user interaction to all managed eTrust VMs for this eTrust VM-Director. Managed eTrust VMs will have chosen eTrust VM-Director as their source for content updates.

CA never "pushes" code or content to eTrust VM-Director. eTrust VM-Director initiates all communication and issues the requests for information. Communication between eTrust VM-Director and CA requires a License Key, which is used to verify that the requesting unit is a valid and active eTrust VM in order for that appliance to receive updates.



Only an Administrator has access to the Maintenance functions. The Maintenance function addresses the backup and restore procedures and defines the start time to perform code updates on eTrust VM-Director.

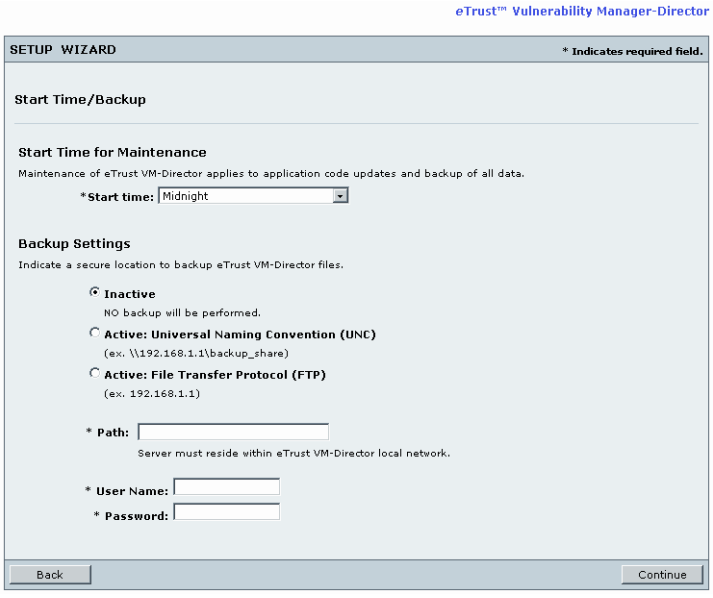
Start Time & Backup

The Start time for Maintenance and the Backup settings may be modified at any time from the Management tab, Start Time/Backup link. Make the necessary changes, then click one of two options at the bottom of the page:

1. **Update**- Updates the settings only. Backup will occur at the scheduled maintenance time.
2. **Update and Backup Now**- Updates the settings and performs a backup when selected.

Start Time

The Administrator will set the time updates will occur. This will be the start time of the maintenance window -- updates will be executed as they become available. The default time is set to 12:00 a.m. ***Because the system will be unavailable during this process, schedule the maintenance for non-business hours.***



Backup Settings

During the set-up process, the user can elect to activate the automated daily backup of files. These settings can also be modified from the Management tab, Start Time/Backup link. The backup **file name** will be auto-generated and be made up of eTrust VM-Director name, code version and a Date/Time stamp. If this option is NOT enabled, back up will not occur.

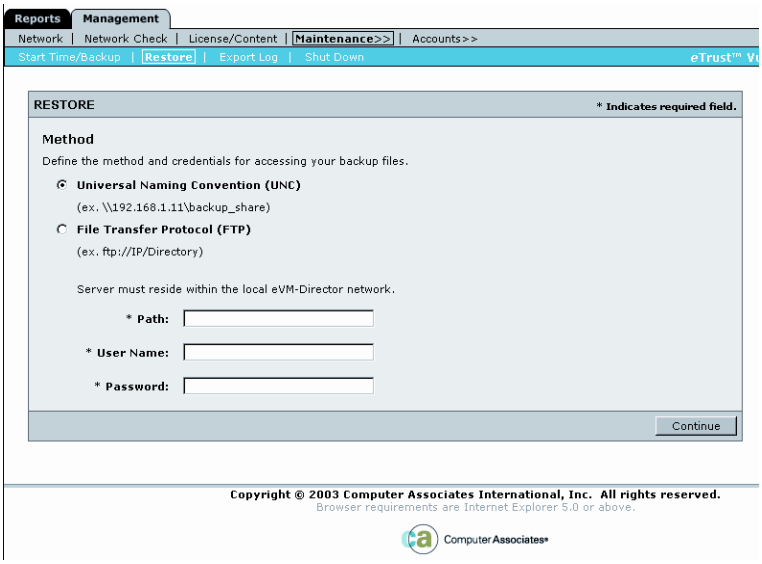
See the Backup Settings section of Setup and Configuration, at the beginning of this User Guide, for complete instructions.

Restore

System restores can be performed on demand. When performing a system restore, users may select from available back-up files. Partial system restores are not permitted. See the Backup Settings for complete instructions.
The Restore function will display a list of all files found on the device identified in the backup information identified above.

Notes:

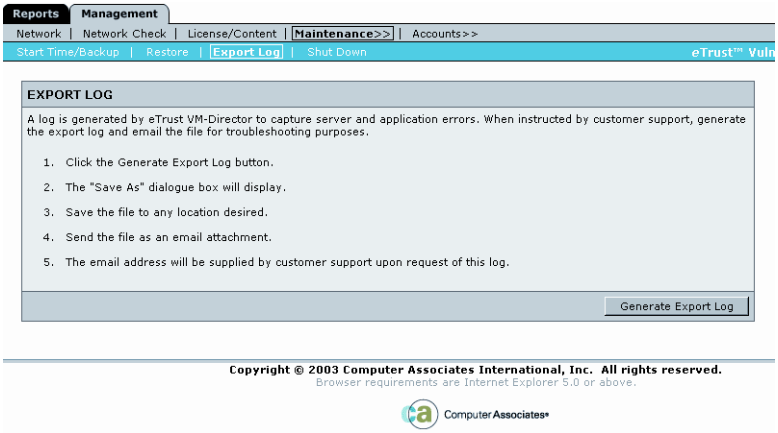
- Partial system restores are not permitted.
- If there is a failure during the restore process, the system will automatically roll back to the state prior to the restore process.
- The user has the ability to change the restore file name, but it is not recommended.
- If the restore process is interrupted, the user name and password for the file location may be locked. This could occur due to the application of network rules. Check with your Network Administrator to verify rules.



Export Log

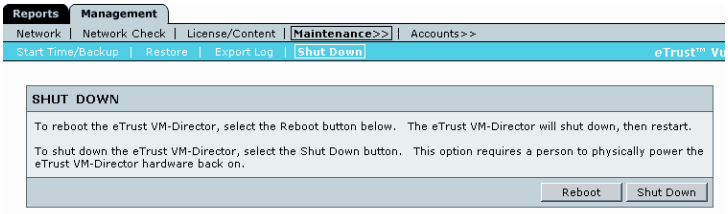
A log is generated by eTrust VM-Director to capture server and application errors. These logs will be used by CA to troubleshoot any difficulties they may have. When instructed by customer support, generate the export log and email the file for troubleshooting purposes. The email address will be supplied by customer support upon request of this log.

1. Click the **Generate Export Log** button.
2. The **Save As** dialogue box will display.
3. Save the file to any location desired.
4. Send the file as an email attachment.



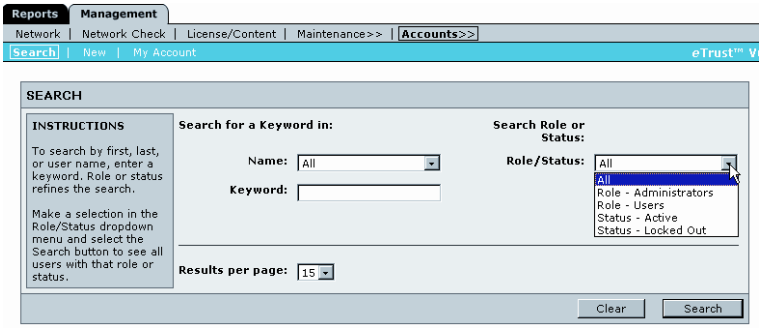
Shut Down

Shut Down will provide a method for an Administrator to shut down or reboot the eTrust VM-Director. The shut down option will require a person to physically power the eTrust VM-Director hardware back on.



ACCOUNTS

The Accounts section of the eTrust VM-Director allows the management of accounts. A maximum of 200 accounts may be created for the eTrust VM-Director, which includes User and Administrator roles. Administrators have access to all User functions, as well as additional administrative functions, including the ability to create and edit user accounts for the eTrust VM-Director. The Accounts link is accessed from the Management tab. Accounts with the role of **User** will not have access to **Search** accounts or to create **New** accounts.



USER ACCOUNT GUIDELINES

- Login names must be unique.
- Login names are NOT case sensitive.
- Only one Role can be assigned to each user account.
- A maximum number of 200 accounts may be created.
- The flag to force password change upon login will automatically be set when a new user account is created or when an administrator changes another account.
- An Administrator account may be deleted if there is at least one other active Administrator account.
- Only the Administrator will have access to create and maintain user accounts with the exception that all users will have access to modify some of their account information.

SEARCH ACCOUNTS

The Administrator can search user accounts. Search criteria includes:

- The name fields (First, Last or Login name) selected from a drop down list. The default is All.
- If one of the name fields is selected then a keyword is required.
- Search by Role or Status, displayed from a drop down list. The default is All.

The Search Results will display the Last Name, First Name, Login Name, Role, Account Status, Created By and Date Created fields for each user in this order.

EDIT AN ACCOUNT

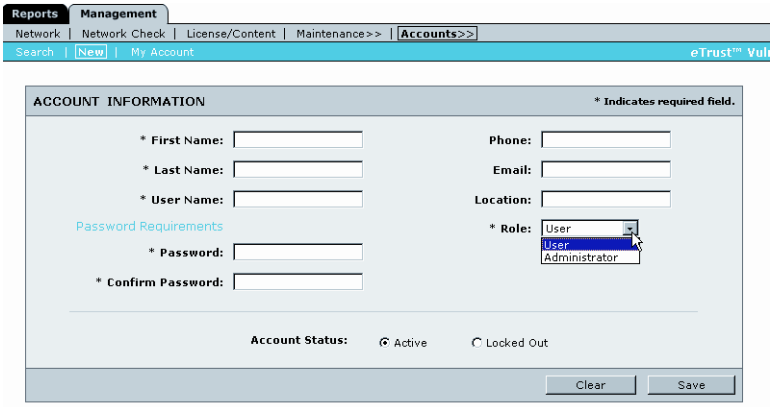
1. Select the **Last Name** link from the list of accounts.
2. The edit form is displayed.
3. Click **Back to User List**, if only viewing this account and no changes are made.
4. Or, click **Delete** to remove this user.

5. The following fields may be modified.
   - First Name and Last Name
   - Password – Click the Password Requirements link as a guide (required field)
   - Confirm Password – Re-type the password
   - Phone – Optional field
   - E-mail address – Optional field
   - Location – Optional field
   - Role – Select the role from the dropdown menu, user or administrator
   - Account Status – By default, the Active radio button will be selected
6. Click **Save** to edit the account.

NEW ACCOUNT

The Administrator role has the ability to create new eTrust VM-Director accounts. Upon login, the user will be prompted to change their password. See the Password Requirements section for guidelines.

1. Click the **New** link from the Accounts menu. The New Account form is displayed.
2. The **First, Last and User name** are mandatory.
3. Create a **password**, according to the mandatory requirements.
4. The **Phone, email and location** of the user are optional.
5. Select the **role** for this account, User or Administrator.
6. The default status will be **Active**. The Administrator can choose to **Lock Out** an account from this screen.

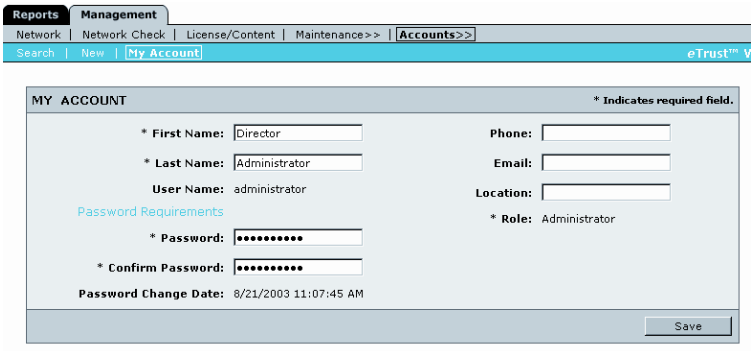


7. Click **Save** to modify, create or delete the account.

MY ACCOUNT

The Administrator, as well as the User roles, has access to **My Account** screen.

1. Click **My Account** from the Accounts menu.
2. Make necessary changes and click **Save**.



FAQS/TROUBLESHOOTING

GENERAL QUESTIONS

Q. What does *e*Trust VM-Director do for me?
A. *e*Trust VM-Director allows the management of multiple eTrust Vulnerability Managers across an organization's network.

Q. What hardware platform runs *e*Trust Vulnerability Manage-Director?
A. *e*Trust VM-Director runs on a Dell PowerEdge 2650, 2.0GHz/512K Cache Xeonn (220-8929).

Q. Who provides technical support?
A. The CA Help Desk [(631) 342-5803 or http://esupport.ca.com] provides Tier 1 support..
Dell covers all hardware with their standard three-year warranty and they will service any hardware failure. Additional detail regarding the warranty and servicing of *e*Trust VM-Director hardware is as follows:

Dell will service any hardware failure. Our agreement with Dell (a Type 3 contract) provides for a three-year warranty with next business day parts and labor. To exercise the warranty, contact Dell regarding any hardware problems—their staff will assist in coordination of any required service or repair (Dell will service hardware onsite).

How to contact Dell for service. To report any hardware issues, contact Dell technical support at 1-800-624-9896. To expedite your service, Dell recommends the following be considered prior to calling:

1. **Before you call Dell:** If you suspect a problem with your system, write down any error messages or beep codes received, if applicable, and perform the diagnostic tests using the Dell Diagnostics Diskette provided with your system. See your system documentation for information about error messages, beep codes and running the diskette-based diagnostics. Document the results of the diagnostic tests.

2. **Talk to a technician:** Be prepared to provide the technician with the following information:
   - Your system's service tag number
   - The names and versions of installed operating systems; the operating system that was running when the problem occurred
   - Peripherals being used
   - Any error messages and/or beep codes received and when they occurred
   - What you were doing when the problem occurred
   - What steps you have taken to resolve the problem, including the results from the diagnostic tests

Q. If my eTrust VM-Director breaks down, what is the process for replacing it?
A. If a severe hardware problem makes your eTrust VM-Director inoperable, Dell will ship you a new unit (or a hard drive with a new image) as early as the next day.

NOTE: You must be using the backup feature for your data to be able to restore the asset profiles, task lists and work history onto the new eTrust VM-Director. If a backup is not available, you must go through the setup process for a "New" *e*Trust VM-Director, rather than a "Replacement" scenario.

Q. While logged in to *e*Trust VM-Director, I was suddenly logged out. Why?
A. Every user may log into *e*Trust VM-Director at the same time. However, the same login name cannot be used concurrently. If another person logs in using the same login name as a user that is already logged on, the first user will be automatically logged out of the application.

Q. I need to change the IP address of the eTrust VM-Director. What implications does this have and how do I change the IP?
A. The eTrust VM-Director IP address can be changed at the Management > Network page. However, this change will significantly impact all associated eTrust Vulnerability Managers. If you change the IP address of an *e*Trust VM-Director, you must also update the configuration settings of all eTrust Vulnerability Managers that are receiving content and code updates through that *e*Trust VM-Director.. If this is not done, code/content updates for those affected eTrust Vulnerability Managers will not be possible.

To change the IP Address of the eTrust VM-Director:
From the Management > Network page, modify the IP Address.

1. Click Save. The machine will reboot.
2. From each eTrust Vulnerability Manager, change the Content Source IP Address for the eTrust VM-Director.

If these steps can be completed *outside* your scheduled maintenance window, the risk of not receiving full updates is minimal. However, if you allow a maintenance window to run before completing all changes, you will encounter content and code update problems. If you will not be able to complete all changes prior to your scheduled maintenance window running, it is strongly recommended that you change the content source for all affected eTrust Vulnerability Managers before changing the eTrust VM-Director IP address. This can be accomplished as follows:

From the eTrust VM-Director home page, Delete the managed eTrust Vulnerability Managers.

1. This will switch the Content Source of each eTrust VM to CA.
2. If those eTrust Vulnerability Managers are connected to the internet, they will continue to receive updates directly from CA.
3. If an eTrust Vulnerability Manager is NOT connected to the internet, no updates will be received.

Q. Does the time schedule for processes in the Management tab automatically compensate for Daylight Savings Time?
A. Yes, as long as the Time, Date and Daylight Savings Time checkboxes are all initially set in the *e*Trust VM-Director Management function. If the *e*Trust VM-Director is using a local network timeserver, the timeserver may or may not compensate.

Q. How do I verify that backups are occurring as scheduled?
A. There are two methods for determining whether the system backups are occurring as scheduled:

1) Access the page Management>Maintenance>Restore. When no backup has been completed, the message at the top of that page will read, "The last restore finished at 8/14/2002 4:24:47 p.m. with a return status of [ERROR]." This page indicates whether a successful backup has been performed on your *e*Trust Vulnerability Manager-Director.
2) The user can check the UNC/FTP location designated for storing the backups. If no files were created during the scheduled backup, then the process did not successfully execute and a backup does not exist (keep in mind any date-time differences that may exist between the *e*Trust Vulnerability Manager-Director and back-up storage device).

SETUP

Q. Why won't *e*Trust VM-Director boot up?
A. Ensure the power cables are plugged into both power plugs.

Q. I can't access *e*Trust VM-Director setup. What could be wrong?
A. If you get a page display error when typing the URL, one of the following may have occurred:

- There are four network jacks in the back of *e*Trust Vulnerability Manager. The jacks are labeled 1 and 2, and the administrative ports are not to be used. The live jack is the one in the NIC added to the second server slots on the right. You cannot connect using any of the other three jacks. Ensure that the network cable is plugged into the NIC 2 slot.
- You may have left out the "s" in the URL (i.e. https://192.168.1.100/).
- Your computer may not be set to an IP address on the same network as *e*Trust VM-Director. This is required to connect through the browser (the default IP address is 192.168.1.100). You may also connect directly to *e*Trust VM-Director with a crossover cable. Utilize the 'ping 192.168.1.100' command at a DOS command prompt to determine if you can communicate to the *e*Trust VM-Director from your computer.

Q. Are there certain browser settings I am required to have?
A. Yes, follow the directions below for configuring Internet Explorer 5.0+ for use with *e*Trust VM-Director..

- Launch Internet Explorer
- Select **Tools**, **Internet Options** from the menu bar
- Select the "**Security**" tab, and then select the "**Custom Level**" button near the bottom of the Internet Options window
- Scroll through the categories and ensure that "enable" is selected for the following settings: **Active Scripting** and **Scripting of Java Applets**
- Click "**OK**"
- Go to the "**Advanced**" tab, scroll down to the **Security** category and ensure **SSL 3.0** is checked
- Click "**OK**"

Q. Can I use Netscape to access *e*Trust VM-Director?
A. No. The only browser application supported by *e*Trust VM-Director is Internet Explorer version 5.0+..

Q. Can I use DHCP to assign the IP address to *e*Trust Vulnerability Manager-Director?
A. No, *e*Trust VM-Director requires a static IP address to operate.

Q. What can I do if a "bad" IP address is assigned to the eTrust VM-Director during setup?
A. If you are unable to access the eTrust VM-Director due to an incorrect or duplicate IP address, complete the following steps:

- Change the IP address of your workstation to an IP within the network of the newly assigned eTrust VM-Directors..
- Isolate the network and the workstation by using a cross-over cable.
- From your workstation, type the previously assigned IP address into the browser address bar.
- Login to the eTrust VM-Director using the administrator username and password.
- Run the Network Check from the setup screen. This check will fail, as you are not connected to a network that will allow the system to communicate to the Internet.
- You will be returned to the Network Information setup page. Here you can enter the correct IP address. Press Continue.
- Enter the Route Table information. Press Save & Reboot. The system will now reboot with the new network configurations.
- Remove the cross-over cables and connect the eTrust VM-Director to the network.
- Continue through the setup process as outlined in the Setup Guide.

Q. Will *e*Trust VM-Director authenticate through a firewall proxy to the Internet?
A. Yes, *e*Trust VM-Director currently authenticates through a firewall proxy. An *e*Trust VM-Director "Administrator" (one of the persons assigned the user role of Administrator in *e*Trust VM-Director) must enter the proxy server's URL (with the port number, if applicable), login name, and password. This information is located under the management tab and is accessible in the network settings.

Q. How do I verify *e*Trust VM-Director can access the Internet?
A. During the setup process, the *e*Trust VM-Director administrator will enter the initial network and route table information, and reboot. After rebooting, they will type in the newly assigned eTrust VM-Director IP Address into the browser address bar and login using the administrator username and password. The setup process will take the user to the Network Check from the setup screen. Run the network check. If this check fails, you will be returned to the Network Information and Route Table screens to re-enter the network information. Check the following items:

- If you utilized a cross-over cable when setting up the network information, verify that you have removed the cross-over cable and connected the eTrust VM-Director to the network. Also, verify the eTrust VM-Director IP address has not been duplicated on the network.
- You can also verify the *e*Trust VM-Director has Internet access by disconnecting *e*Trust VM-Director and assigning another Windows 2000 computer with the same IP address, subnet mask, default gateway and DNS server. Test to see if you can access the Internet and if you can ping the gateway and DNS servers. If you can, your *e*Trust VM-Director will also have access to the Internet when connected.
- Some proxies require the port number be specified. On the Network Information setup page, enter the port number after the proxy URL like so: proxy name:X (where proxy name = the proxy URL, and X = the port number. For example, proxyname.ca.com:80.

After updating the Network and Route Table information, click Save & Reboot. The system will now reboot with the new network configurations. Continue through the setup process as outlined in the Setup Guide.

Once the eTrust VM-Director has completed the setup process, an administrator may verify access to the internet utilizing the network check utility at Management > Network Check. This check will test the DNS resolution of the Content Source (either the *e*Trust VM-Director or Computer Associates) and also verify your system's HTTPS connection to the Content Source. If the Network Check fails, go to the Management > Network page to update your network and route table settings. Changing these settings will force the eTrust VM-Director to reboot.

Q. Is the license key input case sensitive?
A. No, the license key field is not case sensitive.

Q. My license is not validating. Now what?
A. It may be possible that you have assigned the eTrust VM-Director an IP address that already exists on the network. In such a case, the system believes that you have network connectivity and the Network Check has passed…however, the license key does not validate. Verify that a duplicate IP address has not been assigned to the eTrust VM-Director. There may also be a problem with the key. If you've verified that the eTrust VM-Director IP is not a duplicate, but your license is still not validating, contact CA Applications Support at (631) 342-5803 or http://esupport.ca.com to have a new key generated and sent.

Q. I have gone through the setup and rebooted *e*Trust VM-Director. For some reason, I can't seem to access it via the new IP Address. Now what?
A. The IP address of the computer you are using must be changed back to a live IP address on the same network as *e*Trust VM-Director. If your computer is not on the same network, then you will not be able to access *e*Trust VM-Director. To verify that you are on the same network as eTrust VM-Director , ping the IP address assigned to eTrust VM-Director .

After the initial network and route table information is saved and the box reboots, the user must connect the eTrust VM-Director to the network to complete the setup. If you utilized a cross-over cable during the initial setup process, verify that you have removed the cross-over cable and that both your computer and eTrust VM-Director are connected to the network.

If the *e*Trust VM-Director has accidentally been assigned an IP address that has already been assigned to another computer, you will need to connect to *e*Trust VM-Director directly with a crossover cable, log in, reset the network settings with a valid IP address, and continue through the setup process.

CONTENT

Q. How can I verify what version of code *e*Trust VM-Director is running?
A. There are two ways to identify the code version: you check the version displayed on the Home page in the "Release Notes:" field, or the Administrator can access the information on the Management page (the version will be displayed in the shaded box).

Q. How do I know I have pending code that will run during maintenance?
A. The home page "Code:" field reflects "Content Updates: Pending" when there is code that has been downloaded but not yet applied during the maintenance window. When it has been applied, the field will reflect "Content Updates: Current."

Q. I have configured *e*Trust VM-Director and several days have gone by, but I have not yet received a content update. What could be wrong?
A. Check the following:

1) Are there any error messages on the Management > Network Check page indicating problems with connectivity? The *e*Trust VM-Director might not have access to the Internet.
2) When are the code/content updates scheduled? Check the Maintenance screen for the period that the *e*Trust VM-Director is set to update (Hourly or Daily).

Q. My *e*Trust Vulnerability Manager-Director was offline during the scheduled update. Will I get all the updates I need during the next scheduled update?
A. Yes. Code and content updates are referenced by sequence numbers. The next time the *e*Trust VM-Director connects with the server for an update, all information in previously missed sequences will be delivered. Using this method, code and content updates are time-independent (meaning time zones and Daylight Savings Time have no impact on delivery of content).

Q. Can I download content on-demand?
A. Content/code updates cannot be made "on-demand," but the schedules for when the updates occur can be adjusted to run at the next hour. See the Maintenance section of the User Guide or Helpfiles for instructions on how to change the timeframes for code/content update and maintenance window.

Can't find what you're looking for? If you can't find an answer to your question in the FAQs, the rest of the User Guide or in the Helpfiles, contact CA Applications Support at (631) 342-5803 or at http://esupport.ca.com.