eTrust

Getting Started

eTrust Vulnerability Manager

Setup Guide

Computer Associates®

eTrust

To setup eTrust Vulnerability Manager, you will need:

1. Network cables and network connectivity
2. An eTrust VM Host Name
3. A static, available IP Address and Subnet Mask with Internet connectivity
4. The IP Address of the Default Gateway, DNS and Proxy Servers, with login credentials, if applicable
5. The License Key
6. A laptop, PC or server with IE 5.0 or higher installed to access eTrust VM.

Computer Associates®

Setup Overview

1. **Plug in network cable** to the add-in NIC on far left, plug power cord **into jack "1"** and turn on power.
2. eTrust VM **default IP Address is 192.168.1.100**, subnet mask of 255.255.255.0.
3. **Connect to eTrust VM**, set your computer IP to 192.168.1.101 and **enter the URL** of eTrust VM 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 eTrust VM is rebooting, **reconfigure your computer to a live IP address** within the same network as the newly configured IP of the eTrust VM.
6. After reboot, **access eTrust VM 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.

Computer Associates®

STEP 1: Establish Connectivity With eTrust Vulnerability Manager (eTrust VM)

1. Mount eTrust VM on a rack in accordance with the hardware vendor instructions.
2. At the back of eTrust VM, plug in a live network cable to the add-in NIC on the far left side of the appliance, as shown in the image. **DO NOT use the internal default NICs, labeled "1" and "2," or the internal management NIC.**

3. Plug power into eTrust VM, using **power jack "1**.".
4. The default IP Address and Subnet Mask of eTrust Vulnerability Manager will be pre-configured at:
   IP Address – 192.168.1.100, Subnet Mask – 255.255.255.0
5. Connect eTrust Vulnerability Manager 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 eTrust VM 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 eTrust VM from a machine connected to a temporary network. This temporary network can be a crossover cable, connecting eTrust VM 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 to the configuration machine, turn on the power to boot up eTrust VM.

To set up eTrust VM 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 eTrust VM

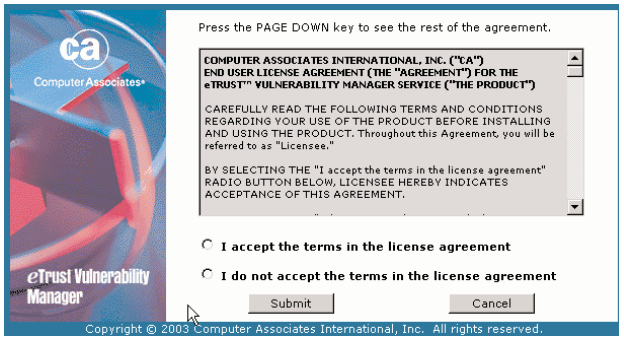
7. Launch an Internet Browser (IE5.0 and higher) from a computer connected to the same network as eTrust VM with a 192.168.1 IP address.

8. Enter the URL (https://192.168.1.100) of eTrust VM into the Address Bar. Upon initial connection, a Security Alert certificate is displayed. Accept the certificate to continue.The License Agreement will be displayed.

Computer Associates®

License Agreement Page

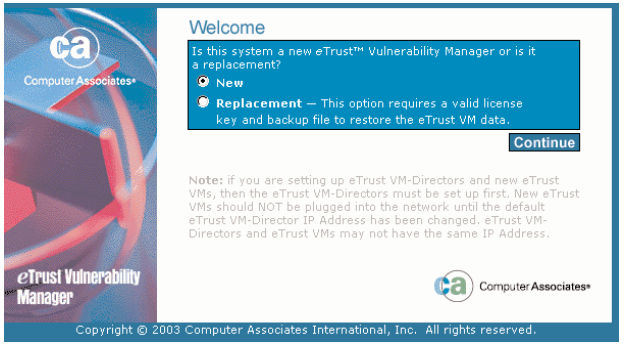
From the License Agreement page, scroll down to view the entire agreement. **Accept** the agreement and click **Continue**.



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.



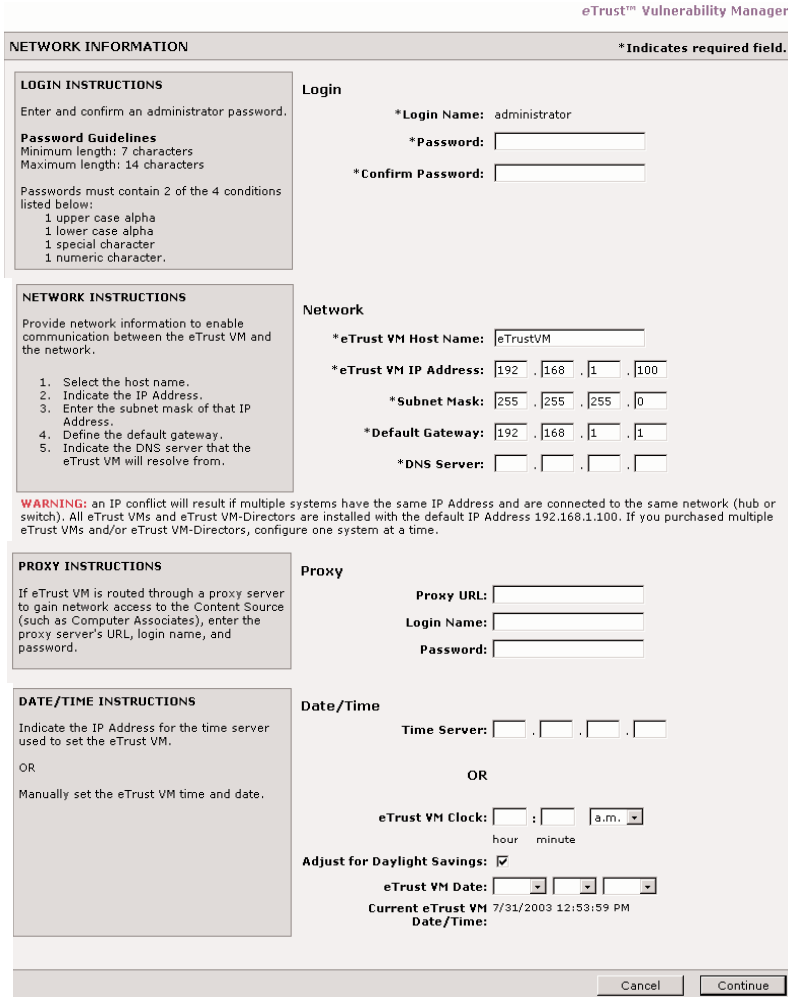
Note:

All eTrust VMs are shipped with same default IP address. To avoid IP conflict during multiple setups, configure one eTrust VM before plugging the next one into your network.

Computer Associates®

STEP 2: Login and Network Information

1. Create a password for the default administrator username and record for future use.
   a. **Guidelines:** 7-14 char, 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 eTrust VM network settings.
   a. Enter the eTrust VM Host Name.
   b. Reconfigure eTrust VM with an IP Address that resides within your network. This IP address will be used to access eTrust VM at the conclusion of Step 2.
   c. Enter the Subnet Mask, Default Gateway, and DNS Server IP addresses associated with the eTrust VM IP address.
3. (Optional) If a Proxy server is used to access the Internet, enter the URL and the login credentials, if applicable.
4. If your network uses a time server, enter the time server's IP address, otherwise set the eTrust VM Clock to the current time.
5. Click **Continue** to display Route Table Settings.



Note:

Record eTrust VM Network Information

Password_____

Host Name_____

IP Address_____

Subnet Mask_____

Gateway_____

DNS Svr_____

Proxy URL_____

6. (Optional) Provide Route Table information

   To Add Network Routes:

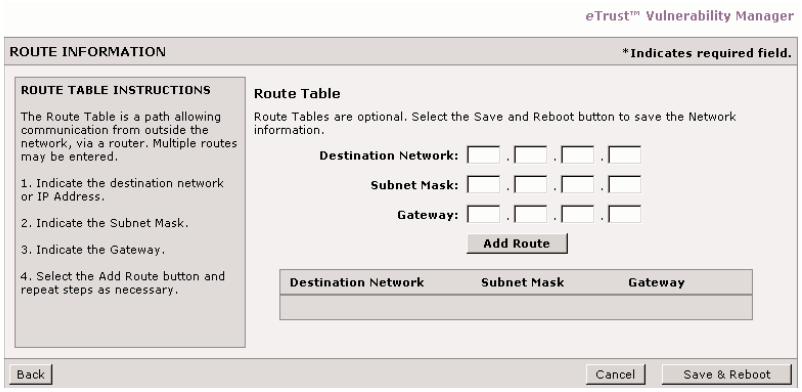
   a. Indicate the IP Address of the destination host or network.

   b. Indicate the Subnet Mask for the destination network.

   c. Indicate the next-hop Gateway for the destination network.

   d. Click **Add Route** and repeat steps as necessary.

   e. Click **Delete** to remove a route.



6. When network settings are complete, click **Save and Reboot**. The reboot process takes up to 8 minutes.

STEP 3: Re-connect to the eTrust VM

1. While eTrust VM is rebooting, reconfigure your machine to an appropriate IP address within the network of the newly assigned IP address of eTrust VM.

2. After eTrust VM reboots, connect to it from your browser-enabled computer. If the machine has been continuously connected to the network, the reboot page will display a link to the new IP address saved in the Network Settings. Otherwise, enter the new eTrust VM URL (e.g. https://10.1.1.100) in the browser's address bar to finish configuration.

Computer Associates®

Note:

If an eTrust VM-Director is being used to manage this eTrust VM, the eTrust VM-D *must* be configured first.

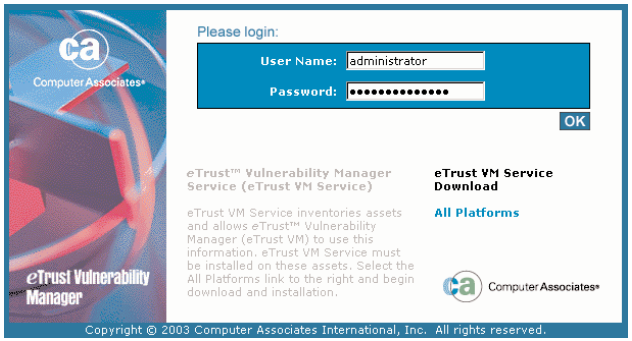
Computer Associates®

3. 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 eTrust VM.

   If the check passed, the Login screen will be displayed.

4. Login to eTrust VM using the login name "administrator" with the password created.



5. For New eTrust Vulnerability Managers: After the login process, eTrust Vulnerability Manager will automatically initiate the **Setup Wizard**. Instructions continue with STEP 4.

6. For Replacement eTrust VMs: See the Restore section on the last page of this guide.

Note:

If the network assigned to eTrust VM requires the use of a proxy for Internet connections, the firewall must be modified to allow the eTrust VM IP address access to the Internet through *port 443*.

Troubleshooting

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

--The eTrust VM 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 eTrust VM.

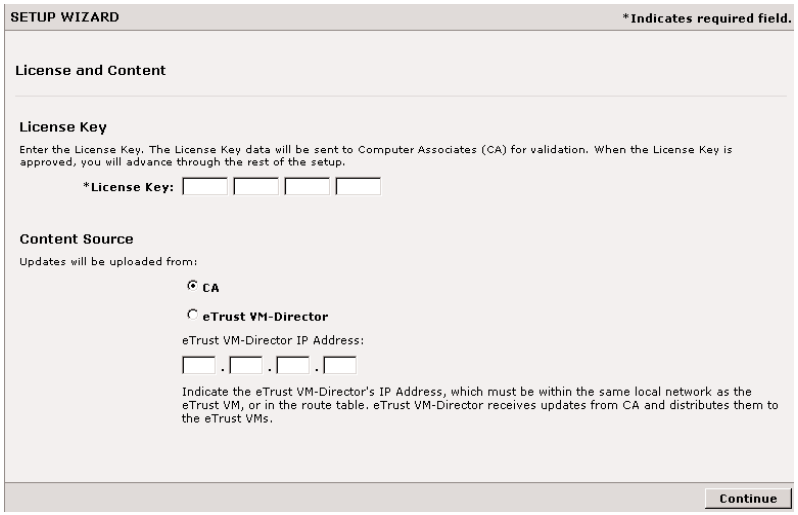
--The eTrust VM IP Address is invalid or not assessable from your network. Take the following action:

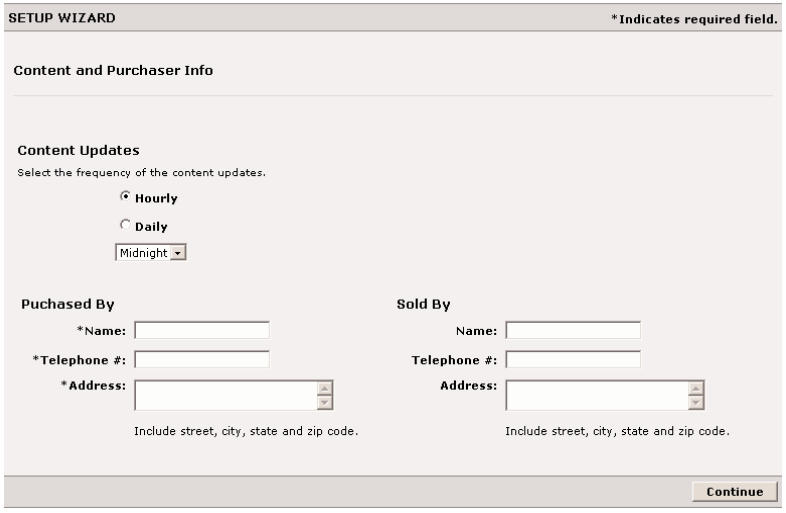
1. Change the IP of your workstation to an IP within the network of the newly assigned eTrust VMs IP.
2. Isolate the network of the eTrust VM and the workstation by using a cross-over cable.
3. Type the previously assigned IP address into a browser address bar.
4. From the Management Tab > Network >>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

STEP 4: Setup Wizard

Step 4a: License Key, Content Source, and Purchase Information

1. Enter the **license key**. eTrust VM must have Internet connectivity in order to validate the license key.
2. Select the **source for content** updates. If you are using eTrust-Director, indicate the appropriate IP address.
3. Select the **frequency** for updates to occur, daily or hourly. If daily, select the time of day.
4. Click **Continue** to validate the license key and proceed with operational settings.
5. Provide the **Purchased By** information for registration purposes. This information will be used solely for user support, content subscription and software maintenance renewal purposes.
6. (Optional) Provide Information identifying the Seller of this eTrust Vulnerability Manager.
7. Click **Continue** to proceed.





Computer Associates®

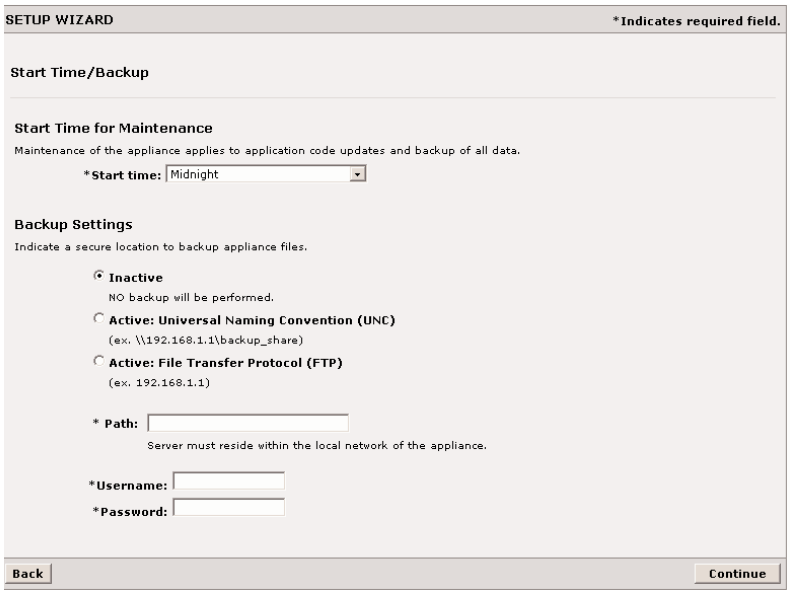
Note:

These settings may be changed under the Management tab in eTrust Vulnerability Manager.

Computer Associates

Step 4b: Maintenance

Maintenance of eTrust Vulnerability Manager refers to code updates to the application and backup of data. See the **Maintenance** section of the User Guide, accessed from the Helpfiles, for more details.



1. Select the time of day to initiate maintenance of eTrust VM (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.

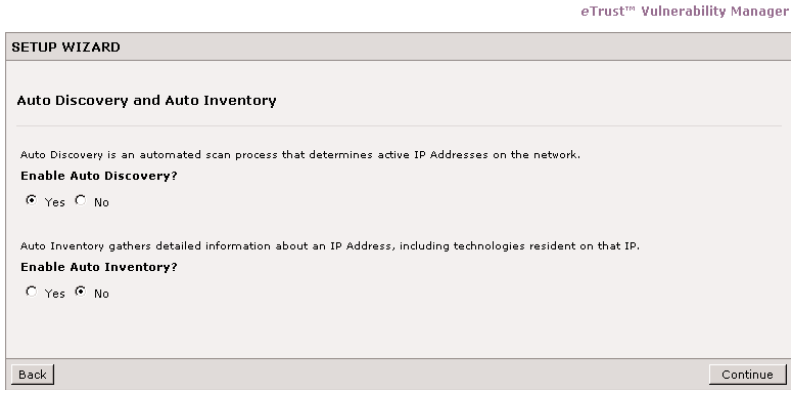
Note:

Maintenance for eTrust VM should be scheduled for non-business hours if possible, as eTrust VM will not be accessible at the time code is applied.

Step 4c: Auto Discovery and Auto Inventory

The Auto **Discovery** process detects devices (assets) on the network. The Auto **Inventory** process generates a detailed list of technologies on assets with an installed inventory service.

1. Select the Radio Button **Yes** to enable both processes. The Wizard will present screens requesting appropriate settings for each process when you continue.
2. Click **Continue** to assign settings for each process.

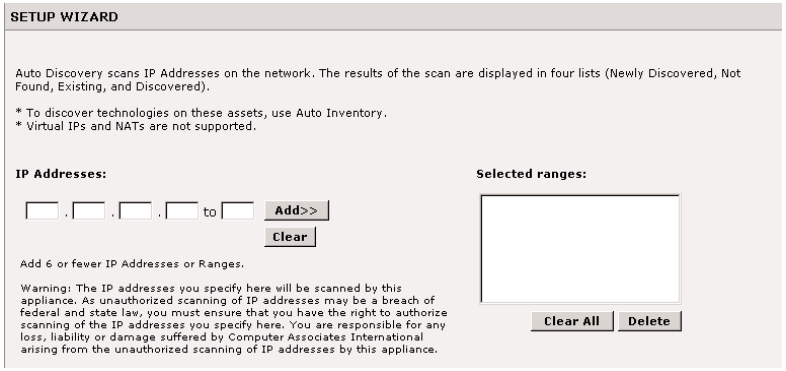


Computer Associates®

Step 4d: Auto Discovery Settings

Auto Discovery provides for the initial discovery of assets and the subsequent monitoring of specified IP ranges, and is best used to quickly input network devices.

1. Enter each IP address range to scan, and click **Add**.
2. Repeat for up to six IP addresses or ranges.
3. To delete an address or range, highlight the address(es) in the “Selected Ranges” box and click **Delete**. Click **Clear All** to delete all addresses/ranges.

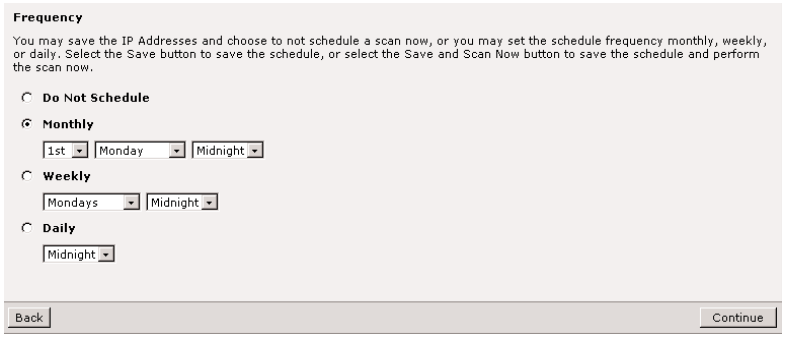


Note:

If the IP Address ranges are not known at this time, the settings can be defined later, from eTrust VM.

Computer Associates

4. Select the frequency for the discovery scan (daily, weekly or monthly).
5. Click **Continue**. The initial scan will be performed at the next occurrence of the scheduled time.



Step 4e: Auto Inventory Settings

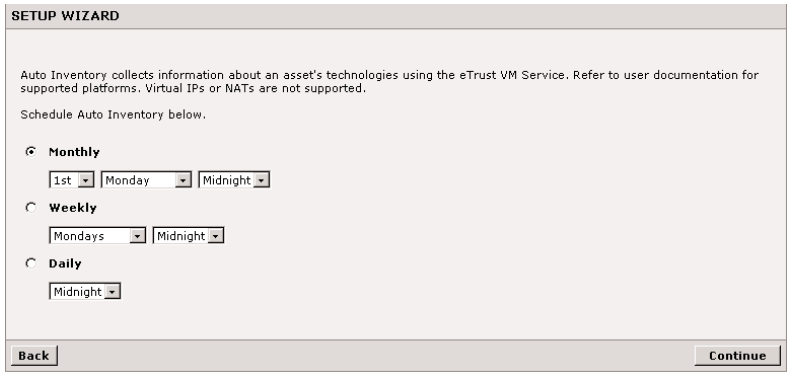
Note:

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

Auto Inventory depends on information provided by the eTrust Vulnerability Manager Service. The service must be installed on the target assets for Auto Inventory to function (see the Service Installation section of this guide).

1. Select the frequency for the inventory of technologies from the service (**hourly, weekly or monthly**).
2. Click **Save** to save the schedule and proceed.

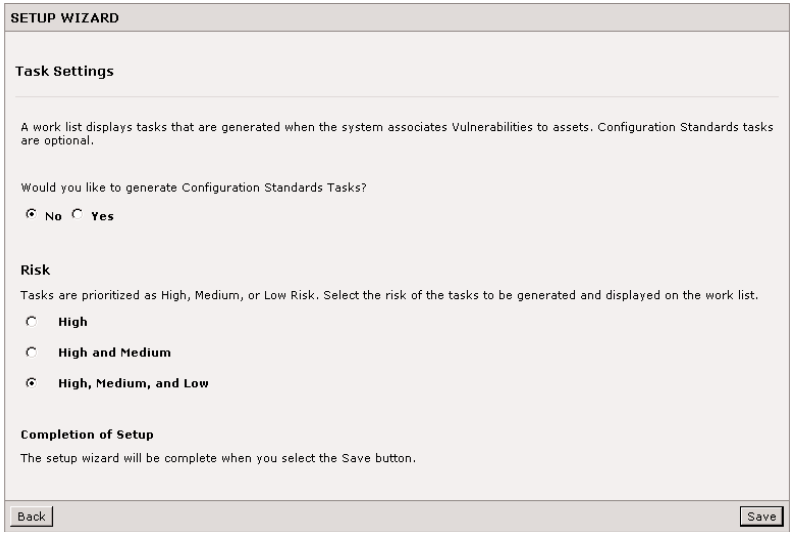
Virtual IP's and NAT are not supported.



Step 4f: Task Settings

eTrust Vulnerability Manager generates an action plan of vulnerability tasks based on your managed assets. Configuration standard tasks are optional.

1. Select **Yes** to include configuration standard tasks.
2. Select the risk category of vulnerability and configuration standard tasks to be included in all work plans.
   a. Indicate **High** to see only high risk vulnerabilities and configuration standards in the work plans. The Wizard defaults to include all tasks (High, Medium, and Low).
3. Click **Save** to proceed.



Computer Associates

STEP 5: Complete the Configuration

After completing all information in the Setup Wizard, click **Save**. The settings will be saved to the eTrust Vulnerability Manager.

The login screen is displayed and you are now ready to deploy the service and manage your assets.

Note:

If an error occurs at the last screen, the appropriate page is displayed for correction. All other entered data is saved.

Computer Associates

eTrust Vulnerability Manager Service Installation

The Auto Inventory process is dependent on the **eTrust Vulnerability Manager Service** being installed on each asset where an inventory of technologies is requested. The inventory service is a program that runs in the background and contains a set of instructions allowing communication between that asset and eTrust Vulnerability Manager. See the eTrust Vulnerability Manager Service section of the User Guide or the Helpfiles for more details.

Methods for installing the service:

- Direct users to eTrust VM for download and installation. The service files are accessible from the login page so there is no requirement that users have eTrust VM account privileges.
- Direct users to an internal server for download and installation. Administrators may copy files to internal servers for distribution.
- Local installation by an administrator.
- Email the service executable to be installed by the end users.
- Repackage the installation with a software delivery tool, like Unicenter Software Delivery.

Note:

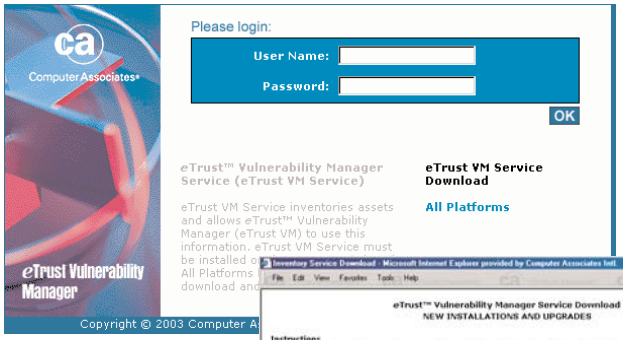
The inventory service is written for specific operating systems. Installation must take place after eTrust VM Setup, to allow the Auto Inventory Process to run properly.

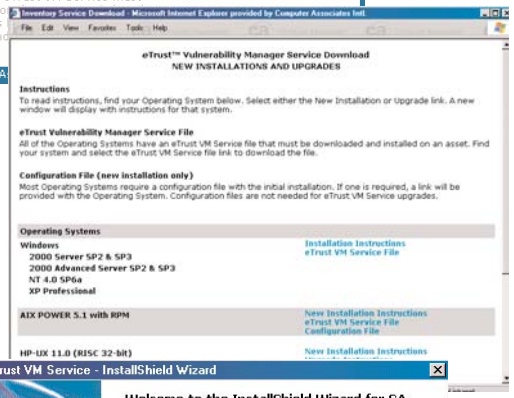
The following Operating Systems are supported for this release:

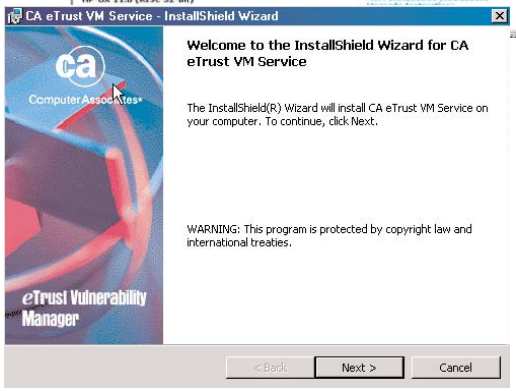
Windows 2000 Server, SP2, SP3, SP4
Windows 2000 Advanced Server, SP2, SP3, SP4
Windows 2000 Professional, SP2, SP3, SP4
Windows NT 4.0, Server SP6a
Windows XP Professional, SP1
Windows Server 2003 (Standard, Web and Enterprise Editions)
Linux Red Hat 6.2, 7.3 and 8.0 (Intel)
Sun Solaris 8 (UltraSPARC)
HP-UX 11.0 (RISC 32-bit)
AIX POWER 5.1 with RPM

Install the Service on Windows

The eTrust VM Service installation for Windows is provided as a standard Microsoft Install (MSI) package. The installer is accessed from the eTrust VM login screen or from the Auto Inventory tab, the **eTrust VM Service** link.







1 Access the eTrust VM Login screen by typing the eTrust VM IP Address in a browser address bar.

2. Click **All Platforms** in the eTrust VM Service Download section to display download links for the install package and the configuration file.

3. Click **eTrust VM Service File** under the Windows section to download the InstallShield Wizard installer file.

4. From the **Save As** dialogue box, download the “CA eTrust VM Service.msi" file to any location.

5. When the file download is complete, click **Open** from **Download Complete** dialogue box. The installer will launch and the Microsoft Installer will begin the program install process.

6. Follow the step-by-step instructions, clicking **Next** to continue. If this is an upgrade, the previous configuration will be automatically detected, and installation will skip to step 9.

Computer Associates®

Note:

Version 2 of the Windows Installer (InstMsiW.exe)must be installed prior to installing the Service on the following Windows OS:

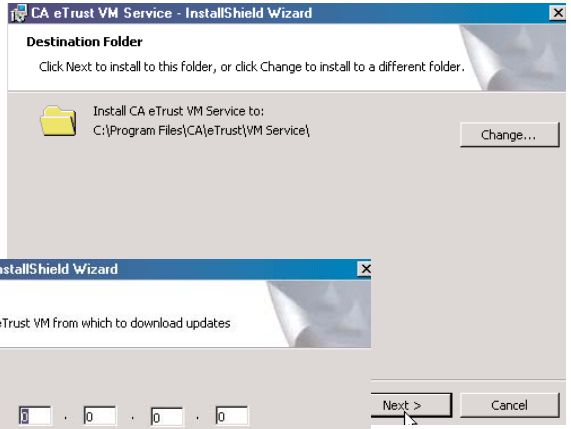
2000 Server,
2000 Advanced Server
2000 Professional,
NT 4.0 SP6a

The file can be downloaded at:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=4B6140F9-2D36-4977-8FA1-6F8A0F5DCA8F

Computer Associates

7. From the **Destination Location** screen, the wizard indicates the location where the service files will be installed. The default location is: C:\Program Files\CA\eTrust\VM Service.
8. Click **Next** to continue.
9. Input the eTrust VM IP address and click **Next** to start the installation process. The status of the install will be shown on the next screen.

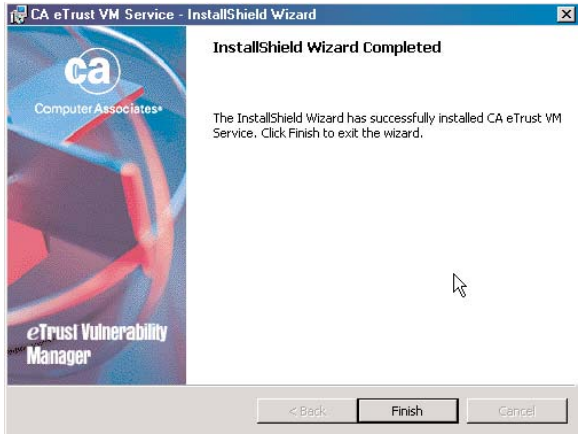


If the IP Address of the eTrust VM is changed at a later date, the service must be modified. See the User Guide or Helpfiles for complete instructions.

Note:

Ensure the correct IP Address is input at this time. If an incorrect IP is input, which cannot be accessed from this box, an error will display.

10. From the last screen, click **Finish**.
11. During the setup process, the Configuration File will be automatically downloaded and populated with eTrust VM settings. The service will run automatically, based on the scheduled time.
12. The eTrust VM Service Installation is now complete.



Computer Associates®

After the eTrust VM Service is installed on the systems, the communication must then be **Enabled** from eTrust VM in order for the Service commands to continue to send data to eTrust VM, such as the technologies on that IP Address. See the Auto Inventory section of the User Guide or Helpfiles for complete instructions.

Computer Associates®

Install the Inventory Service on Solaris

The eTrust VM Service installation for SOLARIS 8 (UltraSPARC) is provided as a package file. Package installation requires root permissions, so these instructions assume the user is running with root privileges.

1. To download the package file:
   a. Access the eTrust VM Login page (IP Address of eTrust VM) using Netscape.
   b. Click **All Platforms**.
   c. Click **eTrust VM Service file** under the Solaris section.
   d. Save the package file to any directory.

2. Install the package file with the following command: pkgadd -d <name_of_file> caevms

   where name_of_file =the full name, including directory path, used to save the package file. For example, if the file was saved in /tmp then the name_of_file, = /tmp/caevms.1.0.0.package.

3. After installation of the package file, download the Configuration File from eTrust VM Login page by clicking the Configuration File link under the Solaris section (see step 1).

4. After downloading the configuration file, copy the file to the eTrustVMS directory with the following command: cp <name_of_file> /etc/CA/eTrustVMS/caevms.crypt

5. After the configuration file is copied to the eTrustVMS directory, the caevms daemon must be manually started to begin the eTrust VM Service scan. After the initial installation, the daemon will run automatically whenever the system boots to multi-user mode.

6. Start the daemon with the following command: /etc/init.d/caevms start

7. The caevms daemon is now running and can be controlled with the /opt/CA/eTrustVMS/bin/caevmsctl program. For more information on caevmsctl see its "man" page. The man pages for caevms and caevmsctl are installed in the /usr/local/man tree. It may be necessary to add /usr/local/man to the MANPATH environment variable to view these pages.

Solaris Requirements:

Minimum run level required - multi-user with networking.

If using a browser to download the files, Netscape must be used.

If using FTP, binary mode must be used.

8. To continue successful use of the eTrust VM Service, assets must be created or managed from the eTrust VM, Assets > Auto Inventory > eTrust VM Service screen. See the IAuto Inventory section of the User Guide for complete details.

NOTE:

If the wget or curl utilities are installed on your system, download and install the configuration directly with one of the following commands:

wget https://{eTrust VMIP}/Agents/config.asp -O /etc/CA/eTrustVMS/caevms.crypt

curl -k https://{eTrust VMIP}/Agents/config.asp > /etc/CA/eTrustVMS/caevms.crypt

(Older versions of curl do not need the -k option.)

Install the Inventory Service on Red Hat Linux

The eTrust VM Service installation for Red Hat Linux 6.2, 7.3 and 8.0 (Intel) is provided as two Red Hat Package Manager (RPM) files, one for Red Hat 6.2 and one for Red Hat 7.3 and 8.0. RPM installation on Red Hat Linux requires root permissions, so these instructions assume the user is running with root privileges.

1. To download the RPM file:
   a. Access the eTrust VM Login (IP Address of eTrust VM) page using Netscape.
   b. Click **All platforms**.
   c. Click **eTrust VM Service** file under the Red Hat Linux section, for the specific release.
   d. Save the RPM file to any directory.

2. Install the RPM with the following command: rpm --install <name_of_file>

   where name_of_file =the full name, including directory path, used to save the RPM file.
   For example, if the file was saved in /tmp, then the name_of_file, = /tmp/caevms-1.0.0-1.i386.rh6.rpm or /tmp/caevms-1.0.0-1.i386.rh7.rpm

Red Hat Requirements:

Minimum run level required - multi-user with networking.

If using a browser to download the files, Netscape must be used.

If using FTP, binary mode must be used.

Computer Associates

3. After installation of the RPM file, download the Configuration File from eTrust VM Login page by clicking the Configuration File link under the RedHat Linux section (see step 1).

4. After downloading the config file, copy the file to the eTrustVMS directory with the following command:
   cp <name_of_file> /etc/CA/eTrustVMS/caevms.crypt

5. After the config file is copied to the eTrustVMS directory, the caevms daemon must be manually started to begin the eTrust VM Service scan. After the initial installation, the daemon will run automatically whenever the system boots to multi-user mode.

6. Start the daemon with the following command: /etc/rc.d/init.d/caevms start

7. The caevms daemon is now running and can be controlled with the /opt/CA/eTrustVMS/bin/caevmsctl program. For more information on caevmsctl see its "man" page.

Note:

The following library version combinations are required for the eTrust VM Service.

Redhat 6.2 with RPM 3.x

Redhat 7.3 with RPM 4.x

Redhat 8.0 with RPM 4.x

8. To continue successful use of the eTrust VM Service, assets must be created or managed from the Assets > Auto Inventory > eTrust VM Service screen. See the Inventory section of the User Guide for complete details.

NOTES:

If the wget or curl utilities are installed on the system, download and install the configuration directly with one of the following commands:

wget https://{eTrust VMIP}/Agents/config.asp -O /etc/CA/eTrustVMS/caevms.crypt
curl -k https://{eTrust VMIP}/Agents/config.asp > /etc/CA/eTrustVMS/caevms.crypt
(Older versions of curl do not need the -k option.)

Install the Inventory Service on HP-UX

The eTrust VM Service installation for HP-UX 11.0 (RISC 32-bit) is provided as a SD-UX depot file. Package installation on HP-UX requires root permissions, so these instructions assume the user is running with root privileges.

1. To download the depot file:
   a. Access the eTrust VM Login page (IP Address of eTrust VM) using Netscape.
   b. Click the **All platforms** link.
   c. Click the **eTrust VM Service file** link under the HP-UX section. .
   d. Save the depot file to any directory.

2. Install the package file with the following command: swinstall -s <name_of_file> caevms

   where name_of_file =the full name, including directory path, used to save the depot file.
   For example, if the file was saved in /tmp then the name_of_file, = /tmp/caevms.1.0.0.depot

3. After installation of the depot file, download the Configuration File from eTrust VM Login page by clicking the Configuration File link under the HP-UX section (see step 1).

4. After downloading the configuration file, copy the file to the eTrustVMS Directory with the following command: cp <name_of_file> /etc/CA/eTrustVMS/caevms.crypt

5. After the configuration file is copied to the eTrustVMS directory, the caevms daemon must be manually started to begin the eTrust VM Service scan. After the initial installation, the daemon will run automatically whenever the system boots to multi-user mode with networking.

6. Start the daemon with the following command: /sbin/init.d/caevms start

7. The caevms daemon is now running and can be controlled with the /opt/CA/eTrustVMS/bin/caevmsctl program. For more information on caevmsctl see its "man" page.

Computer Associates®

HP-UX Requirements:

Minimum run level required - multi-user with networking.

If using a browser to download the files, Netscape must be used.

If using FTP, binary mode must be used.

Computer Associates®

8. To continue successful use of the eTrust VM Service, assets must be created or managed from the eTrust VM, Assets > Auto Inventory > eTrust VM Service screen. See the Auto Inventory section of the User Guide for complete details.

NOTES:

If the wget or curl utilities are installed on the system, download and install the configuration directly with one of the following commands:

wget https://{eTrust VMIP}/Agents/config.asp -O /etc/CA/eTrustVMS/caevms.crypt
curl -k https://{eTrust VMIP}/Agents/config.asp > /etc/CA/eTrustVMS/caevms.crypt

(Older versions of curl do not need the -k option.)

AIX Requirements:

Minimum run level required - multi-user with networking.

If using a browser to download the files, Netscape must be used.

If using FTP, binary mode must be used.

Install the Inventory Service on AIX

The eTrust VM Service installation for AIX POWER 5.1 (with the rpm.rte package installed) is provided as a backup file (bff) in installp format. Package installation on AIX requires root permissions, so these instructions assume the user is running with root privileges.

1. To download the backup file:
   a. Access the eTrust VM Login page (IP Address of eTrust VM) using Netscape.
   b. Click the **All platforms** link.
   c. Click the **eTrust VM Service file** link under the AIX section.
   d. Save the backup (bff) file to any directory.

2. Install the package file with the following command: installp -Xd <name_of_file> all

   where name_of_file =the full name, including directory path, used to save the backup file.
   For example, if the file was saved in /tmp then the name_of_file, = /tmp/caevms.1.0.0.0.bff.

3. After installation of the backup file, download the Configuration File from eTrust VM Login page by clicking the Configuration File link under the AIX section (see step 1).

4. After downloading the configuration file, copy the file to the eTrustVMS directory with the following command: cp <name_of_file> /etc/CA/eTrustVMS/caevms.crypt

5. After the configuration file is copied to the eTrustVMS directory, the caevms daemon must be manually started to begin the eTrust VM Service scan. After the initial installation, the daemon will run automatically whenever the system boots to multi-user mode.

6. Start the daemon with the following command: startsrc -s caevms

7. The caevms subsystem is now running and can be controlled with the usr/opt/CA/eTrustVMS/bin/caevmsctl program. For more information on caevmsctl see its "man" page.

8. Optionally, you can create a symbolic link from /opt/CA/eTrustVMS to /usr/opt/CA/eTrustVMS to provide a simulation of the eTrust VM Service directory structure for other Unix platforms.

9. To continue successful use of the eTrust VM Service, assets must be created or managed from the eTrust VM, Assets > Auto Inventory > eTrust VM Service screen. See the Auto Inventory section of the User Guide for complete details.

NOTES:

If the wget or curl utilities are installed on the system, download and install the configuration directly with one of the following commands:

```
wget https://{eTrust VMIP}/Agents/config.asp -O /etc/CA/eTrustVMS/caevms.crypt
curl -k https://{eTrust VMIP}/Agents/config.asp > /etc/CA/eTrustVMS/caevms.crypt
```

(Older versions of curl do not need the -k option.)

Computer Associates

Restore

If this setup is a configuration of a replacement eTrust VM, Customer Service must have been previously contacted to reset the License Key.

1. Enter the default eTrust VM IP Address (https://192.168.1.100) into the address bar of a browser.
2. The Welcome Screen is displayed. Select Replacement and click Continue.
3. The Network Information is displayed to reconfigure the new eTrust VM.
4. After Save and Reboot, the License Key screen is displayed. Re-enter the original License Key and click Continue.
5. The Restore Screen is displayed. See the Restore Data Section of the User Guide or Helpfiles for complete instructions.

Notes

Notes