eTrust™ Vulnerability Manager

User Guide
Version 1.0

Computer Associates™

TABLE OF CONTENTS

INTRODUCTION

Computer Associates' eTrust™ Vulnerability Manager is a security management tool designed to manage an organization's security implementation. It enables an organization to implement, monitor and measure the effectiveness of its enterprise security posture.

CA delivers functionality from a browser-based application that resides within the customer's network. The tool requires minimal configuration and set-up, enabling the user to obtain value from eTrust Vulnerability Manager (eTrust VM) almost immediately. The product includes an Auto Discovery process to identify assets within the client organization's network, and an Auto Inventory process to identify asset technologies. This functionality enables specific vulnerability identification, as eTrust VM will pull valuable vulnerability and configuration standard data from CA's research database.

eTrust VM can function as a standalone piece of equipment that is installed in a client's network, or it can function in conjunction with eTrust VM-Director™, a tool that allows centralized management of multiple eTrust VMs.

eTRUST VM FUNCTIONALITY OVERVIEW

Auto Discovery

The Auto Discovery process identifies connected devices in the client's network by IP address. Reports are produced that include any additional information that is available, such as Asset Name and Asset Operating System.

Auto Inventory

The Auto Inventory process will retrieve the installed technologies for identified assets within the network and is available for multiple operating systems.

Patch/Fix Application

The application of patch or fix data to an asset will allow the user to indicate for a given technology the patches that have been applied. This feature may be implemented globally or on an individual asset basis.

Global Update of Assets

The Global Update function allows attributes of an asset profile to be globally updated across multiple assets. Attributes to update include: Technology, Patch/Fix, Asset Risk and Asset Function.

Affected Assets List

From Vulnerabilities and Configuration Standards, a link is provided that returns a list of assets impacted by that vulnerability or configuration standard, along with the status of the associated tasks.

Work List

The Work List displays vulnerability and configuration standard tasks. The status of each task is shown and the list can be filtered. All work items are available to any user of eTrust VM.

Work History

Work History displays the history of work items for individual assets. Work items that are no longer applicable to an asset, based on a change in the technology or risk of the asset, or a change in a vulnerability or configuration standard, are archived.

Audit Assessment

Users can develop audit work plans on a per-asset basis. The work plans list work items and allow the user to enter an audit assessment status and notes.

Audit Reports

Audit reports are available that include 1) a detailed listing of an audit assessment, (sorted by asset), and 2) a summary listing, sorted by vulnerabilities/configuration standards.

Content Search

Users may search CA content by vulnerabilities and by configuration standards. Searches are conducted based on keyword, category and/or technology.

Configuration Standard Build Plan

In order to configure a new asset, a configuration standard work plan may be built based on technology and asset function. The system will allow the user to save and modify configuration standard build plans for reuse.

Reporting

The following reports are available:

- ***Vulnerability/Configuration Standards Total Open and Closed*** - reported by asset and by risk.
- ***Vulnerability/ Configuration Standards Risk Status*** - displays number of Open, Closed and the Total, reported by asset, status, and risk.
- ***Vulnerability/ Configuration Standards Summary*** - displays number of assets, number of open and closed work items.
- ***Audit Reports-*** provides the ability to measure compliance.
- ***SANS Top Ten***- lists vulnerabilities and configuration standards that are impacted by the SANS Organization published list of the top ten vulnerabilities for Windows and Unix.

Account Administration

The eTrust VM allows a maximum of fifty User accounts and two Administrator accounts. 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 Vulnerability Manager.

System Back-up and Restore

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

iRecorder Integration

eTrust VM integrates with eTrust Audit by capturing events and mapping them thru iRecorder.

ACCESS CONTROL

There will be two system roles available in eTrust VM:

1. eTrust VM Administrator (Up to two Admin Users)
2. eTrust VM User (Up to fifty Users Accounts may be created, however the system does not support having all 50 users logged on concurrently.

The Administrator role will have access to all functions within eTrust VM. The User will have access to a subset of functions that deal with asset management, auditing and reporting. If it is not stated specifically which role has access to a function, it is implied that it is available to both the Administrator and User.

Communication between users and eTrust VM is accomplished using anonymous SSL. A login process consisting of a user name and password combination is used to authenticate the user. However, the same login name cannot be used in more than one session at a time. If a second user logs in using the same login name as a user already logged on, the first user will be logged out.

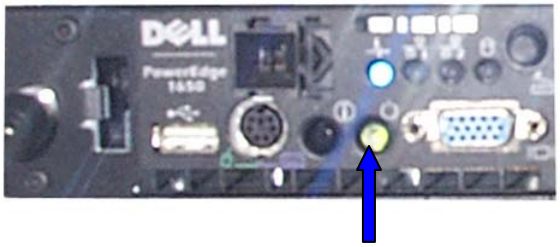
CA never "pushes" code or content to eTrust VM. eTrust VM initiates all communication and initiates the requests for information. A license key is used to verify that the requesting unit is a valid and active eTrust VM. The license key must be valid and current in order for that unit to receive code and content updates.

eTRUST VM CONFIGURATION

CONNECT eTRUST VM TO THE NETWORK

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-on NIC on the far left side of the appliance. **DO NOT use the internal default NICs, labeled '1' and '2', or the internal management NIC.**

3. Plug power into eTrust VM. There are 2 jacks for the power cable. If only **one** power cable is used, power jack **'1' must be used.**
4. The default IP Address and Subnet Mask of eTrust VM will be pre-configured at:
   IP Address – 192.168.1.100
   Subnet Mask – 255.255.255.0
5. Connect eTrust VM 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 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 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, as shown below.



7. Launch an Internet Browser (IE5.0 and higher, or equivalent) from a computer connected to the same network as eTrust VM.
8. Enter the URL (IP Address) of eTrust VM into the address bar (https://192.168.1.100). Upon initial connection, a Security Alert certificate is displayed. Accept the certificate to display the License Agreement.

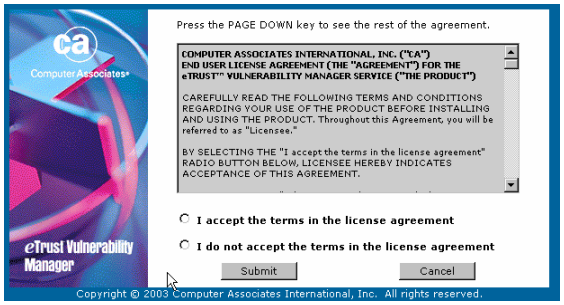
WARNING-an IP conflict will result if more then one eTrust VM has the same IP Address.
All eTrust VMs and eTrust VM-Directors are installed with the same default configuration IP Address of 192.168.1.100. It will create an IP conflict if multiple eTrust VMs or eTrust VM-Ds are connected to the same network (hub or switch).

- If multiple eTrust VMs will be used, configure one system at a time, which will change the default IP Address.
- If an eTrust VM-Director will be used, configure the eTrust VM-D first, then each eTrust VM, one at a time.

LICENSE AGREEMENT SCREEN

To access the eTrust VM, type the URL address into the address bar of an IE browser. eTrust VM is shipped with the default IP Address of 192.168.1.100. The License Agreement page will be displayed.

1. Scroll down to read then entire agreement.
2. Select the radio button to **accept** the terms.
3. Click **Submit**.
4. The Welcome page will be displayed.

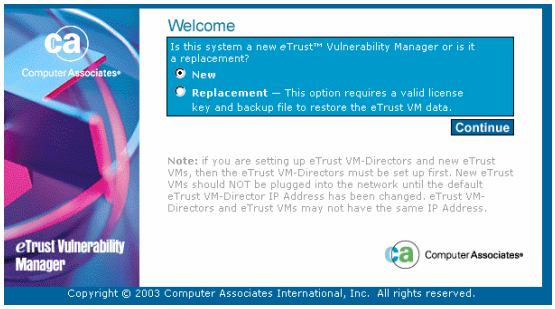


WELCOME SCREEN

After accepting the License Agreement terms, the Welcome Screen is displayed. Choose one of the following:

1. **New** Configuration of this eTrust VM or
2. **Replace** configuration of a previous eTrust VM
3. Click **Continue.**

The Network Information is displayed next.



NETWORK INFORMATION

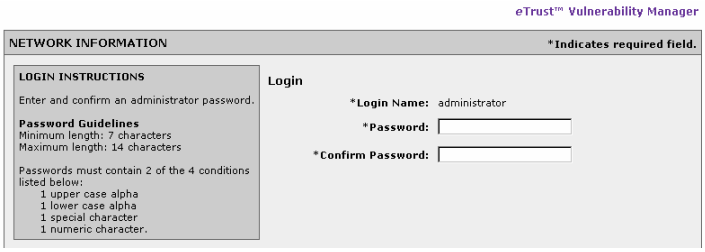
The first screen will gather the following information:

- Login Name and Password
- Network Information (of appliance) IP Address, Subnet, Gateways, DNS Server
- Proxy Server URL and login credentials, if required to access that URL
- Time Settings and Route Table information

Login Name and Password

To Login:

1. eTrust VM is delivered with a default **Administrator** account, which is displayed in the Login Name field.
2. Select a password for the default administrator login name. Retype the password to confirm it.



Guidelines for Setting Passwords

eTrust VM will be delivered with a default Administrator account. Select a Password that meets the following criteria:

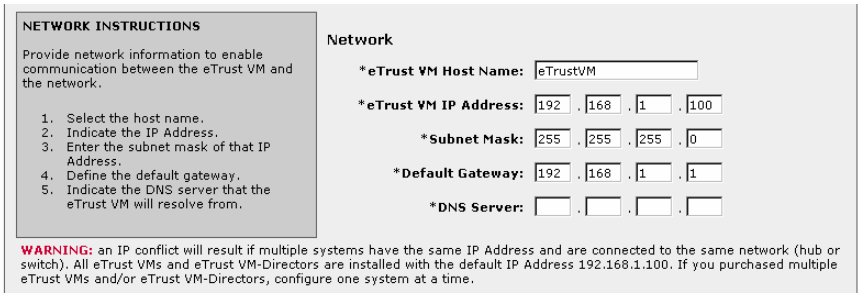
Passwords are case sensitive
Minimum length - 7 characters
Maximum length - 14 characters
Passwords must contain 2 of the 4 conditions listed below:
1 upper case letter
1 lower case letter
1 special character (*,#,!,$, etc)
1 number

- Passwords will not expire and no password history will be kept.
- eTrust VM 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 eTrust VM Administrator or the application will unlock the account after 24 hours has elapsed from the time the account was locked.
- Administrator accounts will be unlocked when eTrust VM is re-booted or powered off/on.
- The session timeout is set to 60 minutes.

Network Addresses

The fields below are used to define the network settings of eTrust VM. The field values are populated with the default settings of the eTrust VM, as shown below. **The IP Addresses MUST be changed** in order to access eTrust VM from your network.

1. Define a **Host Name**.
2. Define the **new eTrust VM IP Address**.
3. Indicate the **Subnet Mask** of that IP Address.
4. Indicate the **default gateway**.
5. Indicate the **DNS server** eTrust VM 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.***

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

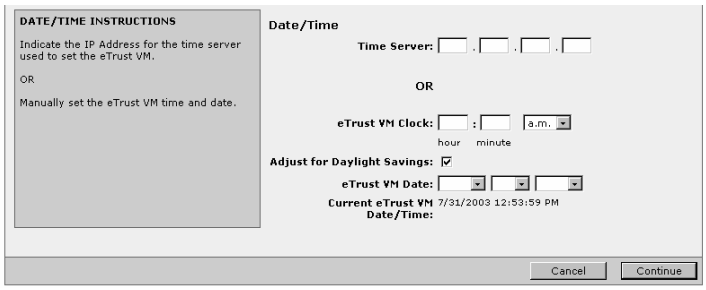
Proxy Server Information

In the Proxy field, indicate the credentials necessary for use of a proxy server. If this URL requires credentials, the login name and password must be indicated.

- The URL is mandatory.
- The login name and password are not mandatory, unless necessary to access the proxy.

eTrust VM Time Server

The last section of the Network Information page determines the time of the eTrust VM.



In the 'Time Server' field:

1. Indicate the IP Address of the time server used to set eTrust VM clock.
   If a timeserver is not used to maintain eTrust VM clock, the clock must be set manually.

To set the clock manually:

1. In the 'eTrust Vm Clock' field, input the time and date.
2. Indicate if Daylight Savings Time should be observed by checking or unchecking the radio button.
3. Click Continue.

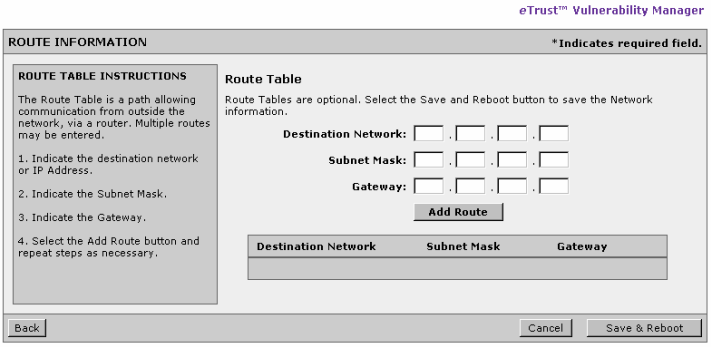
The Route Table information will be displayed next.

Route Table

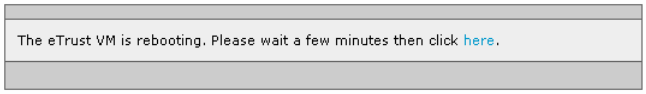
The Route Table is an optional path allowing communication with eTrust VM via multiple paths.

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 the eTrust VM. The reboot process can take up to 8 minutes. After clicking **here**, if a page error is displayed, click the browser 'back' button and allow more time for the reboot.



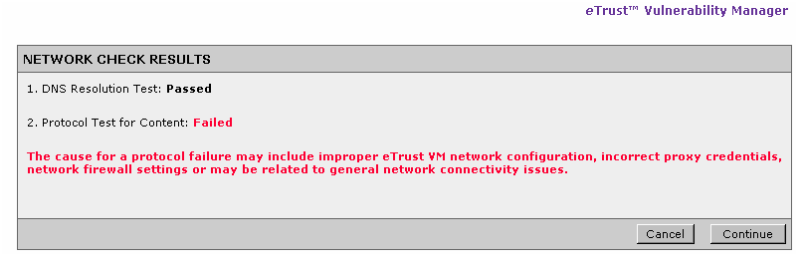
COMPLETING THE CONFIGURATION

1. Change the workstation to an IP Address that is within the newly configured eTrust VM Network.
2. The eTrust VM should take approximately 8 minutes to reboot.
3. After eTrust VM reboots, 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 eTrust VM's new URL (e.g. https://10.1.1.100) in the browser's address bar to finish configuration of eTrust VM.
4. For new eTrust VMs: After the login process, eTrust VM will automatically initiate the **Setup Wizard**. Instructions continue below.
5. For Replacement eTrust VMs: After the login process, eTrust VM will automatically initiate the Restore process. Instructions continue with the Restore section below.

Network Check

After typing the URL (IP Address) into the address bar of the IE browser, the Network Check screen is displayed.

- If the network check **passed**, click continue to begin the setup wizard.
  The login screen is displayed. Login to eTrust VM using the login name "administrator" with the password you created.
- If the network check **failed**, click continue to return to the network page.
  Verify the Network Information entered and correct invalid IPs.
  Continue through the initial setup, following the steps above.



(example of a failed network check)

TROUBLESHOOTING TIPS

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

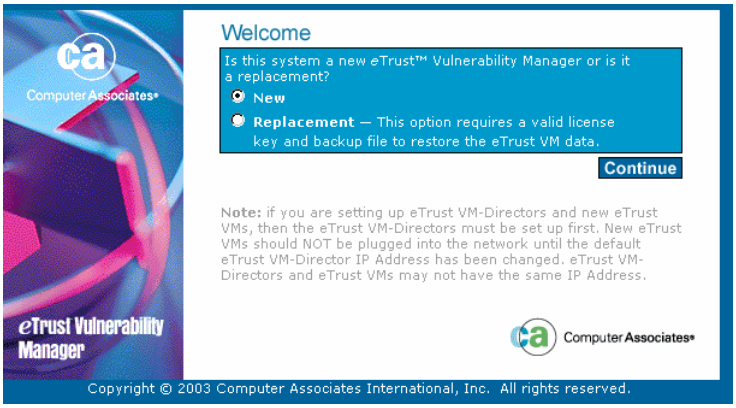
- The eTrust VM has not completed the reboot; wait the full 8 minutes and retry.
- The "**s**" may have been left out of the URL; make sure the **https** is manually entered (e.g. https://1.1.1.1/)
- Your workstation IP address has not been changed back to the same network as eTrust VM. Test this by pinging the new eTrust VM address from your workstation.
- The eTrust VM IP Address is invalid or not accessable 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 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.

RESTORE SCREEN

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 for more information.



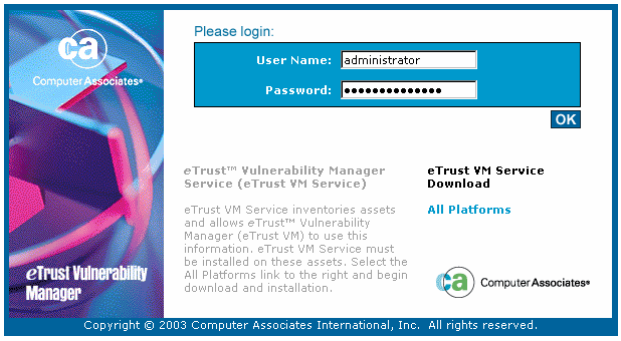
eTRUST VM SETTINGS- SETUP WIZARD

The Setup Wizard offers a step-by-step guide to assist the user in completing the setup. eTrust VM settings are determined at this time, but can be changed, through the Management Tab. The following steps will be completed in the Setup Wizard for eTrust VM:

- License Key validation
- Select source for Content and System Updates – Computer Associates or eTrust VM-Director.
- Purchased by Information
- Maintenance and Backup Settings
- Enable and Define Auto Discovery and Inventory Processes
- Identify Content Type(s) to Include on Work List: Vulnerabilities only or Vulns and Configuration Standards
- Identify Level of Work Items to Include on the Work List (i.e., High, High-Medium, High-Medium-Low)

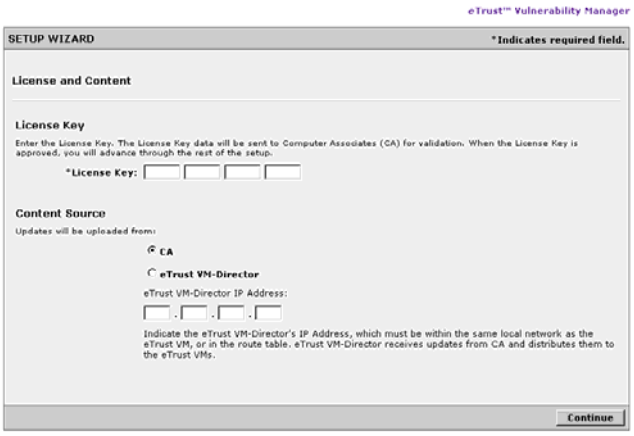
Note: Ensure that the eTrust VM is connected to the Internet during the Setup Wizard process in order to validate the License Key.

After clicking '**Continue'** from the Network Check screen, the login screen is displayed. Type the password that was previously assigned in the configuration steps. The License and Content page is displayed.



LICENSE KEY

Enter the License Key provided for this eTrust VM. The License Key will be validated at the end of the Setup wizard. After validation, this information cannot be modified.



CONTENT SOURCE

If eTrust VM is functioning as a stand alone piece of equipment that is installed on the network, requests for content and code updates will be routed directly to CA via the Internet. If eTrust VM is functioning as part of a "mixed mode" configuration consisting of a eTrust VM-Director that controls multiple eTrust VMs, requests for content and code updates will be made and distributed by eTrust VM-D of the managed eTrust VMs.

1. Select the **source** for requests for Content Updates, from CA or the eTrust VM-Director (CA is selected as the default).
2. Indicate **the IP Address of the eTrust VM-Director**, which must be within the same local network of eTrust VM or in the route table.

NOTE: If a eTrust VM-Director is being used to manage this eTrust VM, the eTrust VM-Director **MUST** be configured first. Change the default IP address of the eTrust VM-Director before plugging any eTrust VMs into the network.

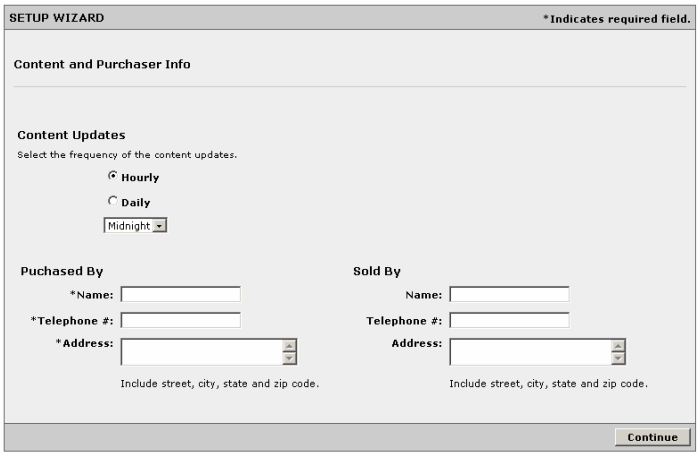
CONTENT/UPDATE SCHEDULE

Content update requests will be issued on either an Hourly or Daily basis, with Hourly being the default.

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

Content and code updates are always initiated/requested by eTrust VM. Content includes:

- Vulnerabilities
- Configuration Standards
- Technologies
- eTrust VM Service Files
- Release Notes
- Messages



PURCHASED AND SOLD BY INFORMATION

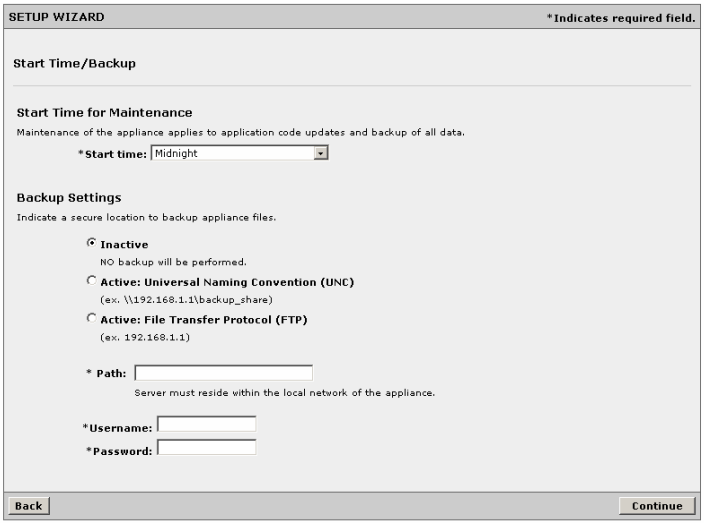
The 'Purchased By' fields are **mandatory**. The 'Sold By' fields are optional.
Click '**Continue**' to validate the License Key and continue to eTrust VM Settings.

MAINTENANCE

Maintenance of eTrust VM applies to code updates to the application and backup of all data. See the Maintenance Section for complete details.

START TIME FOR MAINTENANCE

Content updates were previously scheduled (on the last screen). Those settings indicated a time to initiate communication with CA to send the updates. At that time, the content is downloaded to a holding area, awaiting the scheduled maintenance.



- **Indicate the start time for Maintenance** of eTrust VM, and click **Continue**.

eTrust VM will be down during the maintenance process. Schedule updates for non-business hours.

BACKUP SETTINGS

During the setup process, the user can elect to activate the automated daily 'Backup' of files. If backup settings ARE enabled, eTrust VM database files will be backed up as part of the maintenance process, according to the scheduled time and location (FTP or UNC). Each backup will be a separate file with a new name. If this option is NOT enabled, backup will not occur.

Indicate the location and access information to the appliance file backup. Ensure these access control devices have their ports open to eTrust VM IP.

1. Indicate an **Active UNC** field (ex. \\192.168.1.100\backup_share) **OR** an **Active FTP** field (ex. 192.168.1.100)
2. Enter the **username and password** that allows access to the backup location.

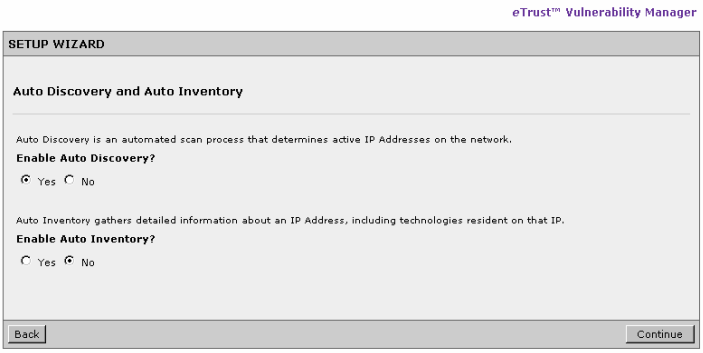
AUTO DISCOVERY AND AUTO INVENTORY SETTINGS

The Auto Discovery process detects devices/assets on the network and the Auto Inventory process sends back an inventory of the technologies on those devices. The information captured via the Auto Discovery and Auto Inventory processes will be transmitted to eTrust VM. Assets can be created or 'Managed' from these results and technologies can by associated to these assets. Tasks related to new or updated information about the asset will be generated (or deleted) as necessary. See the Auto Discovery and Auto Inventory sections for complete instructions.

Enable Auto Discovery and Auto Inventory Processes

During the set-up process, the user can elect to Enable Auto Discover and Auto Inventory processes. The selection of Auto Discovery and Auto Inventory is independent of each other (one or both features can be selected).

- Select the Radio Button (**Yes or No**) to enable one or both. If **Yes** is selected, the Settings for each process will be displayed.



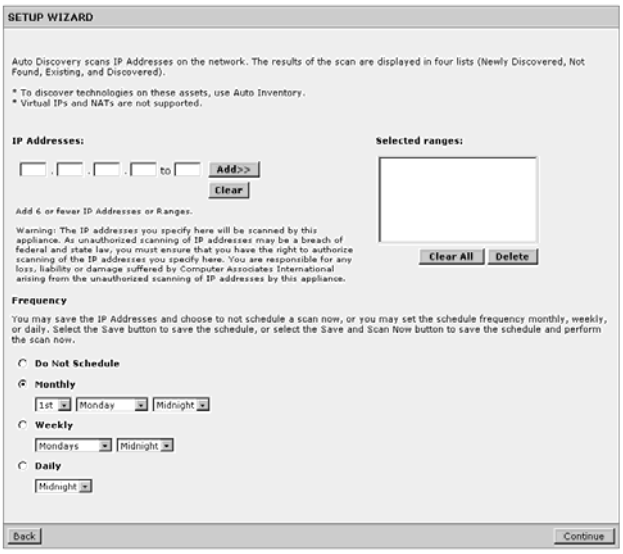
AUTO DISCOVERY SETTINGS

The Auto Discovery settings in the Setup Wizard allow the user to schedule the automated scans. The scan process will scan the entire network of the eTrust VM and determine active IP Addresses.

Set the IP Addresses/Ranges

IP Addresses/Ranges must be within the local network of the eTrust VM, or in the Route Table. Up to 6 single IP Addresses or Ranges may be specified and scanned at one time.

1. Enter one **IP Address, or a Range**, to scan.
2. Click **Add**.
3. To delete an address or range, highlight the address(es) in the **Selected Ranges** box.
4. Click **Delete**.
5. Click **Clear All** to delete all addresses/ranges.



Schedule the Scan

Schedule Auto Discovery scans of the network.

1. Indicate if the scan should run **hourly, weekly or monthly**.
2. If **Monthly** is selected, choose the week, day and time.
3. If **Weekly** is selected, choose the day and time.
4. If **Daily** is selected, choose the time.
5. Click **Continue** to schedule the scan and continue the setup process.

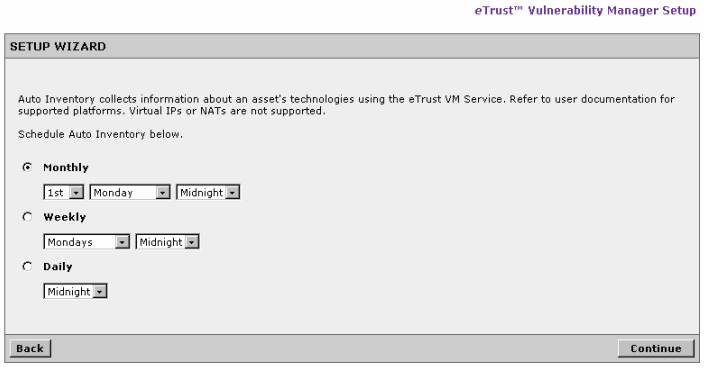
AUTO INVENTORY SETTINGS

Inventory is a list of assets and their technologies returned by the Auto Inventory process. Auto Inventory must be enabled in eTrust VM settings. The eTrust VM Service must be installed on the asset/desktop prior to the Auto Inventory process. Data will be returned from the following operating systems: AIX, HP.UX, Linux-Redhat, multiple Windows platforms, and Solaris. The Auto Inventory process will support DHCP; however, it will not support virtual IPs or NAT.

Schedule the Scan Time

Schedule a new Inventory or modify/delete a previously scheduled Inventory:

1. Indicate if the inventory service should run **hourly, weekly or monthly**.
2. If **Monthly** is selected, choose the week, day and time.
3. If **Weekly** is selected, choose the day and time.
4. If **Daily** is selected, choose the time.
5. Click **Save** to generate the Auto Inventory configuration file and schedule the inventory.

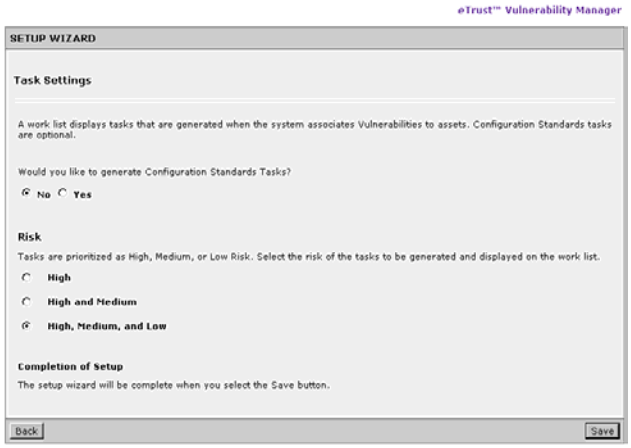


eTrust VM Inventory Service

The Auto Inventory process is dependent on the 'eTrust VM Service' installation on each desktop or device where an inventory of technologies is requested. The service is a program that contains a set of instructions allowing communication between that device and eTrust VM. See the eTrust VM Service Installation section for installation instructions for the supported operating systems. The inventory service is installed after completion of eTrust VM Setup and the files are available from the login page.

Task Settings

eTrust VM provides a work list of tasks generated from the included vulnerability content associated to the managed assets on eTrust VM. Configuration Standard content is also included. However, configuration standard tasks are optional. The Task settings give the user the option to include Configuration Standard tasks in the work list. Tasks are prioritized as High, Medium or Low Risk. The user can designate the risk level of the tasks that will appear on the Work List.



1. Select **Yes** or **No** to indicate if tasks will be generated from configuration standard content associated to your assets.
2. Select the **risk level** of the tasks to be displayed on the work list. (The default is High, Medium and Low)

Each time these settings are changed, the Vulnerabilities and Configuration Standard asset impact analysis will launch. Tasks will be added as necessary. See the Work List section for more information.

Complete Appliance Setup

After completing all information in this setup wizard, click **Continue**. If errors are encountered, the system will retain the entered data and return to the appropriate screen with the error response. After a successful **Save**, the login screen will be displayed. You are now ready to deploy the inventory service and manage your assets.

HOME PAGE

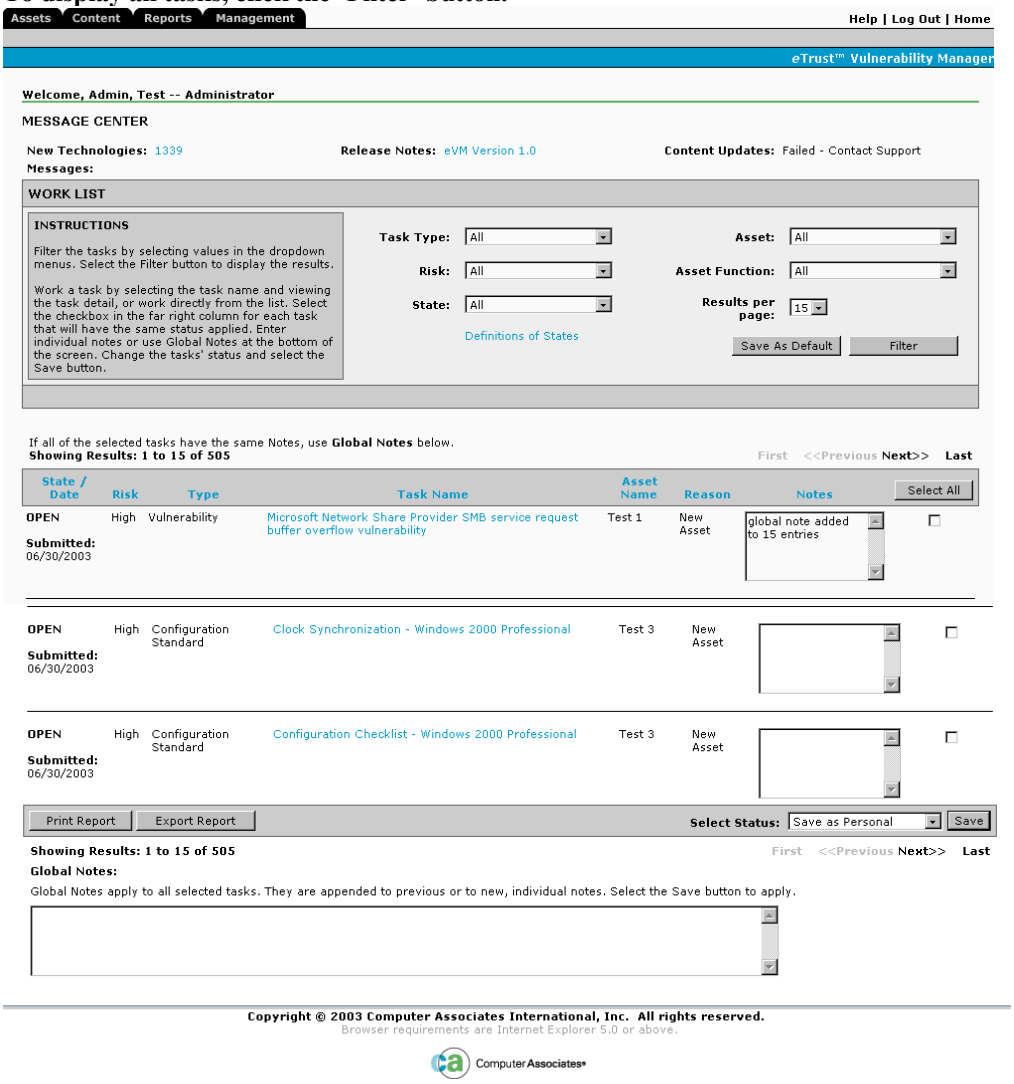
Upon login, the home page will be displayed as shown below. Content within the home page includes:

- 4 Tab Navigation
    1. Assets
    2. Content
    3. Reports
    4. Management

- The Message Center, with links to:
    1. New Technologies
    2. Release Notes
    3. Messages

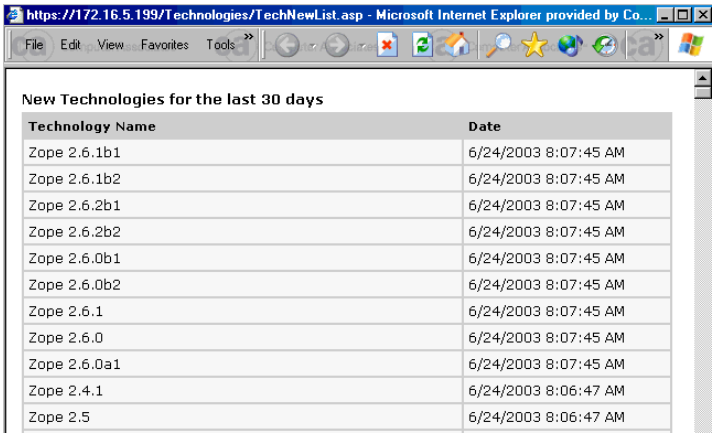
- Content Updates field indicates date of last successful update.
- The User Name and appliance role at the top of the page
- The Work List provides instant access to all tasks on your work list.

To display all tasks, click the 'Filter' button.



NEW TECHNOLOGIES

A link alerts users to new CA-supported technologies that have been added within the past 30 days. The user can add these new technologies to existing assets they may apply to, which will be detected via Auto Inventory. See Associated Technologies for more information.



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 an eTrust VM. Major releases include new functionality or significant enhancements to existing functionality. Minor releases include fixes or patches.

MESSAGES

Messages from CA will be available to users via a link on the home page to inform of miscellaneous information that may not be specific to a particular type of content. For example, it could include notification that the CA content distribution system is going to be down for a period of time or that a new security threat has been released.

CONTENT UPDATES

The 'Content Updates' field on the home page Message Center will display the status of the update process.

AUTO DETECT ASSETS AND TECHNOLOGIES

The Auto Discovery process detects devices/assets and the Auto Inventory process takes an inventory of the technologies on those assets/devices. The information captured via the Auto Discovery and Auto Inventory processes will be transmitted to the eTrust VM. Tasks related to new or updated information about the asset will be generated (or deleted) as necessary.

ENABLE AUTO DISCOVERY AND AUTO INVENTORY PROCESSES

During the set-up process, the user can elect to Enable Auto Discover and Auto Inventory processes. This function can also be enabled in the **Asset Tab, Auto Inventory, Auto Discovery settings**. The selection of Auto Discovery and Auto Inventory is independent of each other (one or both features can be selected). If this option is NOT enabled, neither process will run.

- Select the Radio Button (**Yes or No**) to enable one or both.
- If **Yes** is selected, the Settings for each process will be displayed.

ETRUST VM SERVICE INSTALLATION

The Auto Inventory process is dependent on having the 'eTrust VM Service' installed on each asset where an inventory of technologies is requested. The 'Service' uses a configuration file that contains a set of instructions allowing communication between that asset and eTrust VM. The service runs and sends the data to eTrust VM at the scheduled time. Information included in this configuration file includes:

- IP Address of eTrust VM
- Scheduled Run Time.

The service is written for specific operating systems and the installation must take place after eTrust VM Setup, before the Auto Inventory process can run. The following Operating Systems will be supported for this release:

- **Windows 2000 Server, SP2 and SP3**
- **Windows 2000 Advanced Server, SP2 and SP3**
- **Windows Server 2003**
- **Windows XP Professional**
- **Windows NT 4.0, Server SP6a**
- **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.**

Methods for installing the service:

- Direct users to the eTrust VM for download and installation. The service files are accessible from the eTrust VM 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 service files to internal servers for distribution.
- Local installation by an administrator.
- Email the eTrust VM service package to be installed by the end users.
- Repackage the installation with a software delivery tool, like Unicenter Software Delivery.

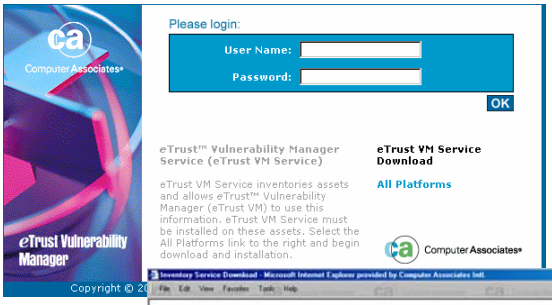
The eTrust VM Service may be installed on all systems, but the communication must be 'Enabled' from eTrust VM in order for the eTrust VM Service commands to send specific data to eTrust VM, such as the technologies on that IP Address. An eTrust VM user will enable the eTrust VM Service communication from the Auto Inventory Results screen by creating or updating an asset. See the Auto Inventory section for more details.

INSTALL THE eTRUST VM 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 login screen or from the Auto Inventory tab (the Inventory Service link) in eTrust VM.

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

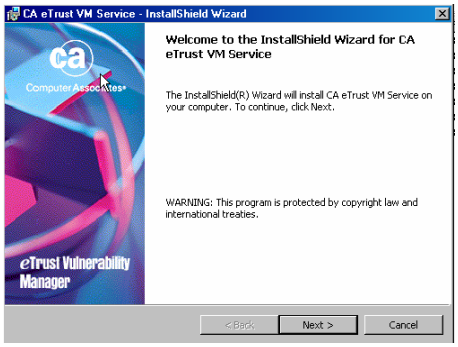
2. Click the **All Platforms** link in the eTrust VM Service Download section to display download links for the install package and the configuration file.



3. Click **eTrust VM Service File** link 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.

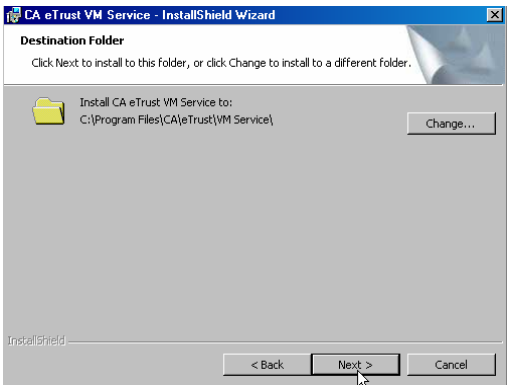
5. When the file download is complete, click **Open** from 'Download Complete' dialogue box. The installer will launch and the Microsoft Installer will begin the program install process. (If the installer does not display and an error is received, so the Upgrade Windows Installer topic below.)



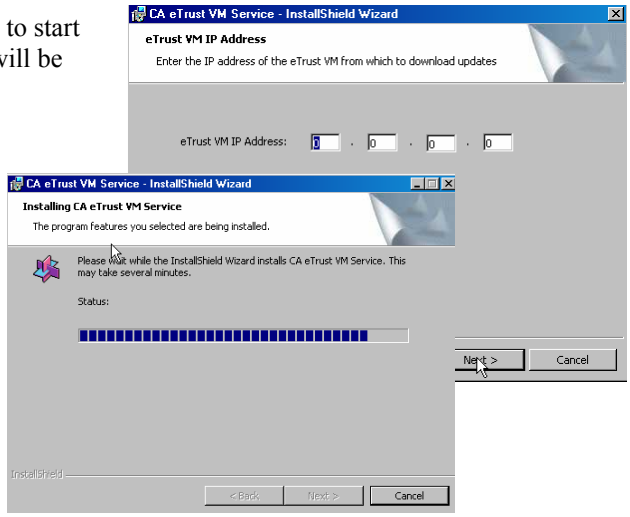
6. Follow the step-by-step instructions, clicking **Next** to continue. If this is an **upgrade**, the previous configuration will be automatically detected, and installation will skip to step 10 below.

7. From the **Destination Location** screen, the wizard indicates the location where the service files will be downloaded. The default location is: **C:\Program Files\CA\eTrust\VM Service**.

8. Click **Next** to continue.

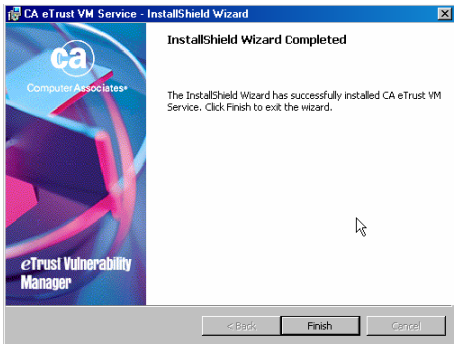


9. **Input the eTrust VM IP address** and click **Next** to start the installation process. The status of the install will be shown on the next screen.



NOTE: Ensure the correct IP Address is input at this time. If an incorrect IP is entered and cannot be accessed from this box, an error will display. If the IP Address of the eTrust VM is changed at a later date, the service must be modified. See the Modify section below.

10. From the last screen, click **Finish**.



11. During the setup process for new installations, the Configuration File will be automatically downloaded. For upgrade installations, the configuration file will be migrated from the previous installation. The file will be populated with information determined from the eTrust VM settings. The service will run automatically, based on the scheduled time.

12. The eTrust VM Service Installation is now complete.

NOTE:
For new installs, the asset will be listed on the Inventory screen and must be created before the next scheduled scan. For upgrades, if this asset has **not** been created in eTrust VM at the time the service runs, no technologies will be returned. Ensure the asset is created before an inventory of technologies is performed.

UPGRADE WINDOWS INSTALLER

Prior to installing the eTrust VM Service for the following Windows OS:

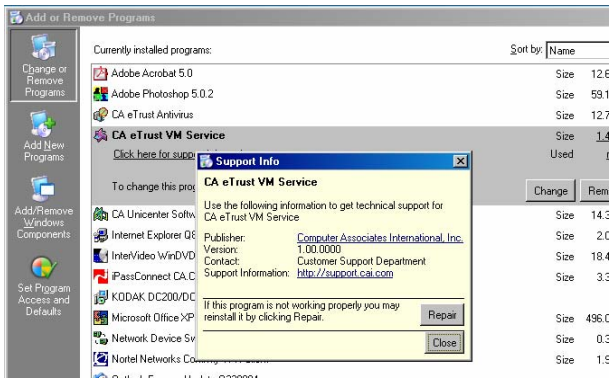
2000 Server
2000 Advanced Server
2000 Professional
NT 4.0 SP6a,

Version 2 of the Windows Installer (InstMsiW.exe) must be installed. This file can be downloaded from:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=4B6140F9-2D36-4977-8FA1-6F8A0F5DCA8F

DETERMINE CURRENT ETRUST VM SERVICE VERSION FOR WINDOWS

To determine the current version of the eTrust VM Service that is running on a system:

1. Go to **Start >>Settings>>Control Panel**
2. Select **Add/Remove Programs**
3. Select **CA eTrust VM Service**
4. Click the **Support Information** link
5. The current version should be **1.00.000**

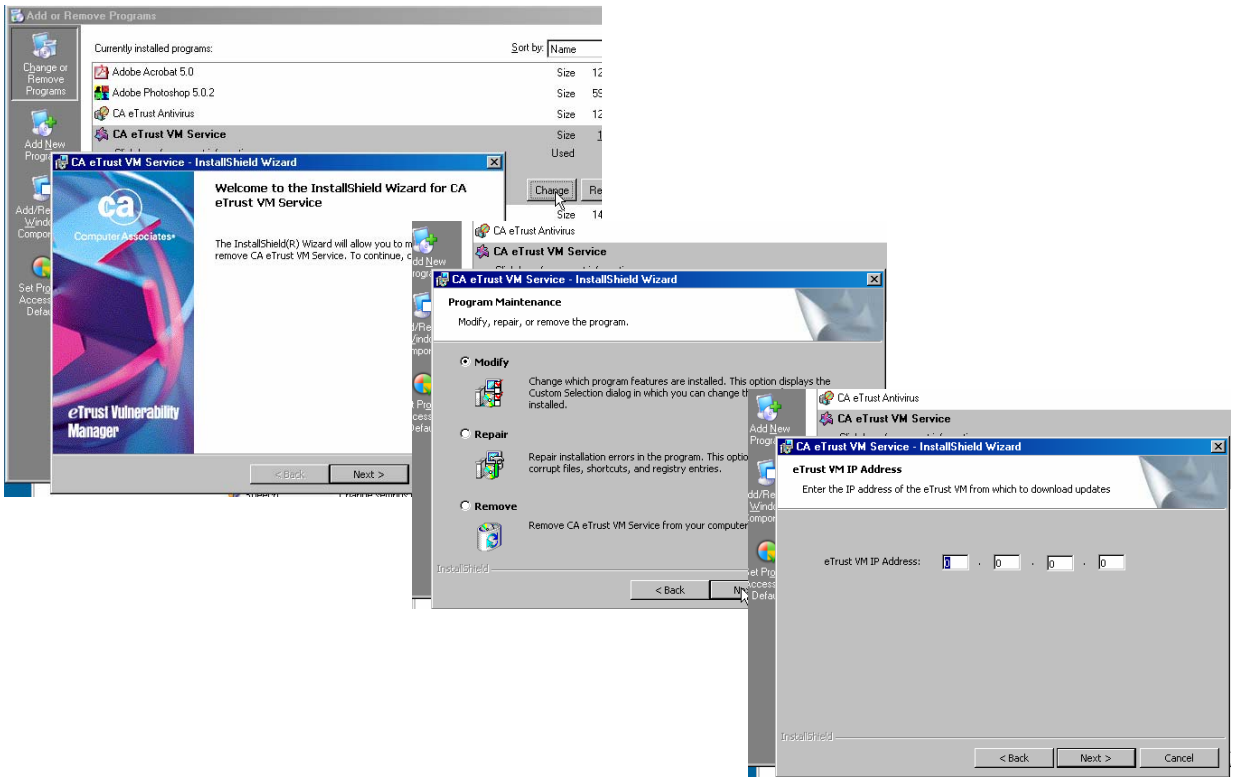


MODIFY THE SERVICE

If the IP Address is changed on the eTrust Vulnerability Manager, the change must also be made on the service installer in order for the technologies to be reported to the proper eTrust VM.

To change the IP Address on the eTrust VM Service:

1. Go to **Start >>Settings>>Control Panel**
2. Select **Add/Remove Programs**
3. Select **CA eTrust VM Service**
4. Press the **Change** button.
5. The Installer will display. Click **Next** to continue.
6. Select **Modify** and click **Next** to continue.
7. Input the new IP Address and click **Next**.



INSTALL THE eTRUST VM SERVICE ON SOLARIS

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

- Minimum run level required is multi-user with networking.
- If using a browser to download the files, Netscape must be used.
- If using FTP, binary mode must be used.

1. To download the package file:
   a. Access the eTrust VM Login page using Netscape. This is the IP Address of eTrust VM.
   b. Click the **All Platforms** link.
   c. Click the **eTrust VM Service file** link 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 by clicking on 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.

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 Inventory section of the User Guide for complete details.

NOTES:
If you have the wget or curl utilities installed on your system, you can 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 eTRUST VM 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. Other requirements:

- Minimum run level required is multi-user with networking.
- If using a browser to download the files, Netscape must be used.
- If using FTP, binary mode must be used.

The eTrust VM Service for Redhat requires specific versions of the RPM libraries to be installed. ***See the Note below.***

1. To download the RPM file:
   a. Access the eTrust VM Login page using Netscape. This is the IP Address of eTrust VM.
   b. Click the **All platforms** link.
   c. Click the **eTrust VM Service file** link 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

3. After installation of the RPM file, download the Configuration File from eTrust VM Login by clicking on the Configuration File link under the RedHat Linux 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 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.

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 Inventory section of the User Guide for complete details.

NOTES:
If you have the wget or curl utilities installed on your system, you can 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.)

The eTrust VM Service requires the following RPM library versions to be installed. If the versions are different then indicated below, they will not be compatible and the Service will fail.

Redhat 6.2 with RPM 3.x
Redhat 7.3 with RPM 4.x
Redhat 8.0 with RPM 4.x
Redhat 9.0 is not currently supported.

INSTALL THE eTRUST VM SERVICE ON AIX

The eTrust VM Service installation for **AIX POWER 5.1 (with the rpm 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. Other requirements:

- Minimum run level required is multi-user with networking.
- If using a browser to download the files, Netscape must be used.
- If using FTP, binary mode must be used.

1. To download the backup file:
   a. Access the eTrust VM Login page using Netscape. This is the IP Address of eTrust VM.
   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 eTrust VM-Dy 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 by clicking on 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 Inventory section of the User Guide for complete details.

NOTES:
If you have the wget or curl utilities installed on your system, you can 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 eTRUST VM 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. Other requirements:

- Minimum run level required is multi-user with networking.
- If using a browser to download the files, Netscape must be used.
- If using FTP, binary mode must be used.

1. To download the depot file:
   a. Access the eTrust VM Login page using Netscape. This is the IP Address of eTrust VM.
   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 on 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/bin/caevmsctl** program. For more information on caevmsctl see its "man" page.

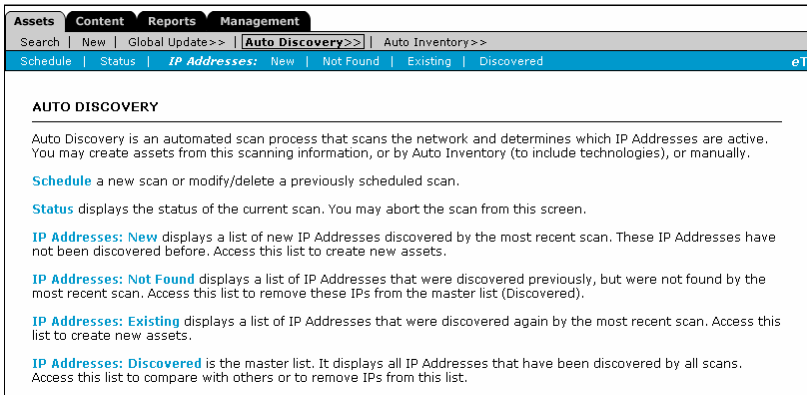
8. To continue successful use of the eTrust VM Service, assets must be created or managed from the eTrust VM, Assets > Auto Inventory > eTrust VM Service screen. See the Inventory section of the User Guide for complete details.

NOTES:
If you have the wget or curl utilities installed on your system, you can 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.)

AUTO DISCOVERY

Auto Discovery is an automated scan process that determines active IP Addresses, or connected devices in the client's network within a specified IP address range. The information can then be used to create Assets. Up to six *Class C* networks may be scanned.



Access control devices (ie. firewalls, packet filtering routers, etc.) must allow communication from eTrust VM to network segments that contain assets for Auto Discovery on the following ports: ICMP echo, 21 (ftp), 23 (telnet), 25 (smtp), 80 (http), 110 (pop3), 111 (rpc), 139 (netbios), 443 (https), 445 (w2k).

For each discovered asset the IP Address will be returned, along with any additional information that is available, such as Asset Name (QDN or Machine Name) and Asset Operating System.

From the Assets Tab, click **Auto Discovery**. Options available from this screen include:

Schedule a Scan
Display the Status of Scans
Display lists of Assets found in a scan.
Manage or Unmanage Assets from scanned lists.

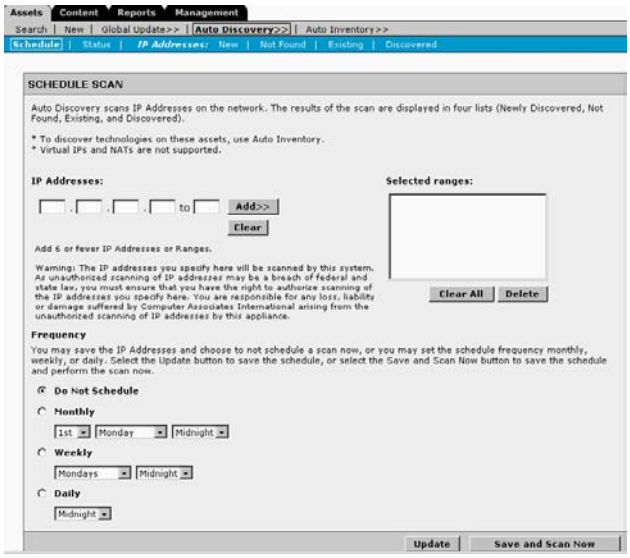
AUTO DISCOVERY SETTINGS

The Auto Discovery settings allow the user to indicate IP Addresses or ranges to scan, and when to schedule the automated scans. **Note**: The IP addresses entered must represent ones that you have full authority to.

Schedule Scan

Schedule a new scan or modify/delete a previously scheduled scan:

1. Display the scan settings from the menu**:** **Assets > Auto Discovery > Settings**.
2. **Indicate the IP Addresses/ranges** to scan. Up to 6 single IP Addresses or Ranges may be specified and scanned at one time.
3. Indicate if the scan should **run hourly, weekly or monthly**.
4. If **Monthly** is selected, choose the week, day and time.
5. If **Weekly** is selected, choose the day and time.
6. If **Daily** is selected, choose the time.
7. Click **Update** to save changes.
8. Click **Save and Scan Now** to initiate the scan immediately. The current time does NOT have to be the same as the Scheduled time.



Abort a Scan

A scan can be aborted at any time and will ignore all data obtained. The message will display the number of IP Addresses scanned out of the number requested. Click the **Abort** button to stop the scan.

RESULTS OF AUTO DISCOVERY SCAN

The results of the Auto Discovery scans will be presented in lists that display information about the IP Addresses found or not found in the scan. The lists are interactive with a master Discovered list and managed by comparison of that list. The four lists produced are:

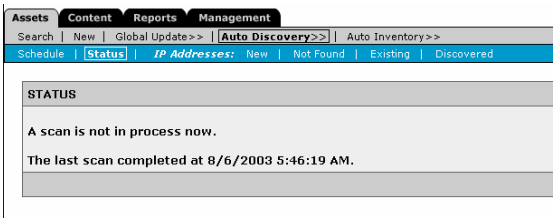
1. Newly Discovered
2. Existing
3. Not Found
4. Discovered

Matching IP Addresses

The IP Addresses found in the Auto Discovery scan will be matched against the IP Addresses of assets in eTrust VM. If there is a match, the Auto Discovery list will indicate that the asset is currently managed in eTrust VM. If no match of IP Addresses is found, the user has the option to create the asset at that time.

Display the Status of a Scan

The Status link in the Auto Discovery menu allows the user to display the status of current and previous scan. The date and time of the last completed scan will display, as well as an indicator on any current scan activity.



CREATE OR MANAGE AN ASSET FROM LIST

Assets can be created or 'Managed' from the 'Newly Discovered' and 'Existing' scan results lists. Click the **Create Asset** link for each asset you would like to manage. This link will only be available for Assets that have a status of **Not Managed**. Each asset must be created individually from this list in order to provide information that could not be obtained in the scan. For more information on creating an Asset, see the Asset Management section.

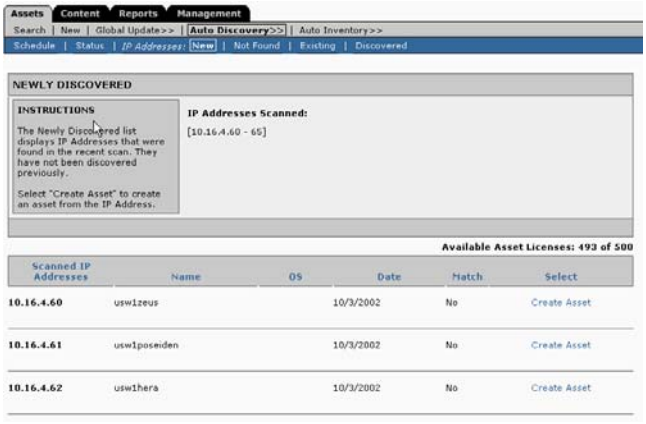
DELETE OR UNMANAGE AN ASSET

An Asset status cannot be changed from 'Managed' to 'Not Managed' status from the scan results lists. The asset must be deleted from the Asset Profile screen. No links will be available for 'Managed' Assets. For more information on deleting an Asset, see the Asset Management section.

Newly Discovered

The **New** link displays a list of new IP Addresses that were discovered by the most recent scan. These IP Addresses have not been discovered before. Access this list to manage these new assets.

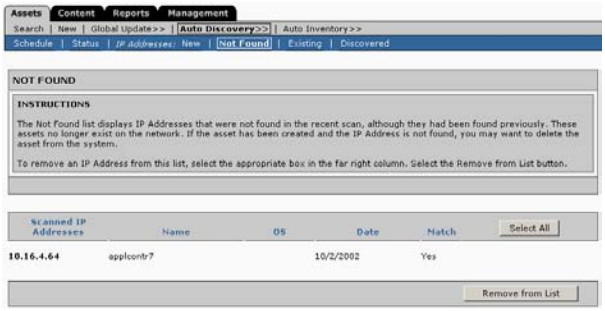
- The list will indicate if a **Match** was found with a currently managed asset.
- From the 'Newly Discovered' list, manage assets by selecting the checkboxes in the right column, then click the **Create Assets** link.
- An asset can be changed to a status of **Not Managed** only by deleting the asset from the Asset Profile screen.



Not Found

The **Not Found** link displays a list of IP Addresses that are on the previously Discovered list, but were not found by the most recent scan. These assets or IP Addresses no longer exist on the network. If this asset was created, but the IP Address can no longer be found, the user may want to delete the asset. Access this list to remove these IPs from the master list (Discovered).

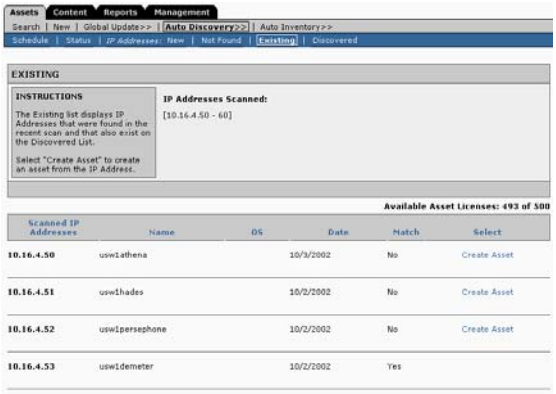
- Delete the asset from the Discovered list by selecting the checkbox, then clicking **Remove From List**.
- A **'Select All'** option is also available.



Existing

The **Existing** link displays a list of IP Addresses that were discovered again by the most recent scan. Access this list to manage assets you have not previously chosen to manage.

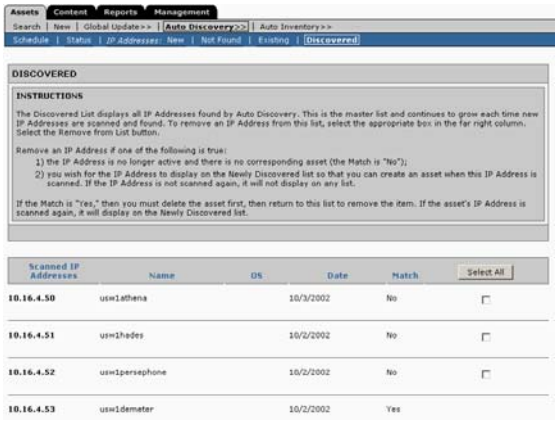
- The list will indicate if a **Match** was found with a currently managed asset.
- From the **Existing** list, manage assets by clicking the **Create Assets** link.
- An asset can be changed to a status of **Not Managed** only by deleting the asset from the Asset Profile screen.



Discovered

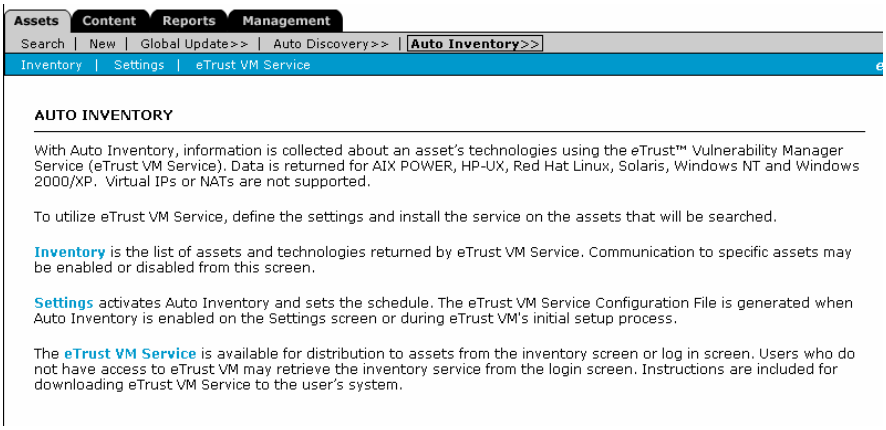
The **Discovered** link displays a list of IP Addresses that have been discovered by all scans. This is the Master List. Access this list to remove IPs from this list.

- Managed Assets must be deleted from the Asset Profile screen.
- Assets may be deleted from this list, only if there is **No Match**.
- To delete, select the checkbox, then click **Remove From List** link at the bottom of the page.



AUTO INVENTORY

Auto Inventory is a process that utilizes eTrust Vulnerability Manager Service Configuration files, installed on assets to gather detailed information about an IP Address, including technologies that reside on these devices/assets. The information captured via the auto inventory process allows users to manage the technologies associated to their assets. Tasks related to new or updated information about the asset will be generated (or deleted) as necessary.



Auto Inventory is supported for the following operating systems:

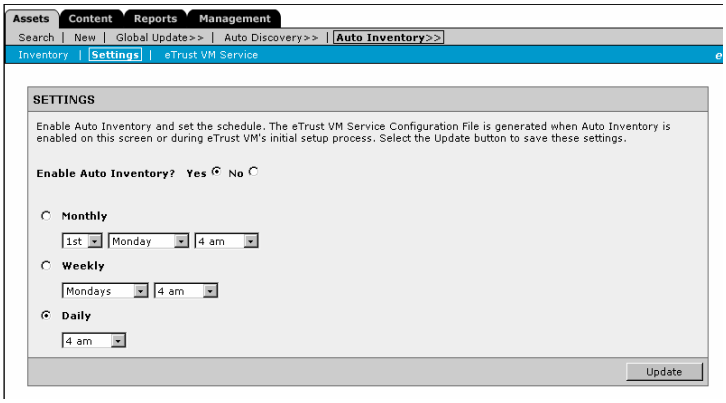
- **Windows 2000 Server (SP1, SP2 and SP3)**
- **Windows 2000 Advanced Server (SP1, SP2 and SP3)**
- **Windows Server 2003**
- **Windows XP Professional**
- **Windows NT 4.0, Server SP6a**
- **Linux Red Hat 6.2, 7.3 and 8.0 (Intel)**
- **Sun Solaris 8 (SPARC)**
- **HP-UX 11.0 (RISC 32-bit)**
- **AIX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

See the Service Installation section for details on each operating system.

AUTO INVENTORY SETTINGS

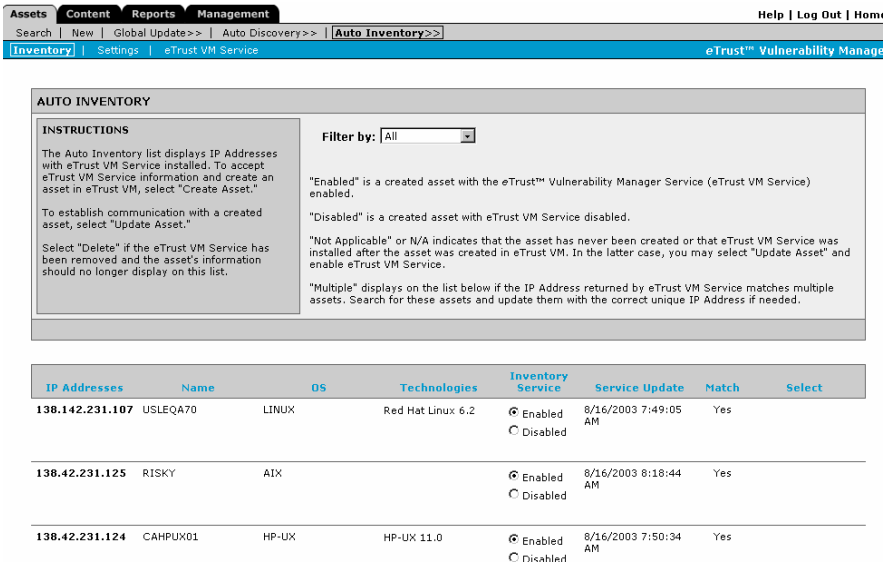
Auto Inventory Settings allows the user to schedule Auto Inventory or to enable/disable the process. The inventory service configuration file is generated when Auto Inventory is enabled on the Settings screen or during the initial setup process.

Select the **Update** button to save these settings.



AUTO INVENTORY RESULTS

The Auto Inventory process displays an inventory of information about the IP Addresses found or not found in the scan. The inventory displays the list of assets and technologies returned by the service. Communication to specific assets may be enabled or disabled from this screen. The list may be filtered by Inventory Service status (enabled, disabled or N/A) and columns may be sorted.



Fields of the display

- **IP Address**-indicates the address of the device/asset
- **Name**- indicates the host name or DNS of the device/asset
- **Operating System (OS)** – indicates the Operating System of that device/asset
- **Technologies**- lists technologies on that device/asset, if the inventory service is enabled
- **Inventory Service**- indicates if the service is enabled or disabled on this IP Address
- **Service Update**-indicates the date when the service last sent data from this IP Address
- **Match**- matches the IP Address sent from the service with eTrust VM asset IP Address to determine if it is a managed asset in the system (Yes or No)
- Select **Delete** to remove that IP Address from the inventory list for non-managed assets
- Select **Create Asset** to manage this asset
- Select **Update Asset** to enable the service and update the technologies on this managed asset.

CREATE AND MANAGE THE ASSETS

The IP Addresses sent from the service on each asset in the Auto Inventory scan will be matched against the IP Addresses of managed assets in eTrust VM.

Inventory Service Status

The list displays these assets and determines the status of the inventory service communication with this IP Address. Inventory Service Statuses are:

- **Enabled** is a created asset with inventory service communication enabled.
- **Disabled** is a created asset with inventory service communication disabled.
- **Not Applicable or N/A** indicates that the asset has never been created or that the inventory service was deployed after the asset was created. In the latter case, you may select "Update Asset" and enable the inventory service.
- **Multiple** displays on the list below if the IP Address returned by the inventory service matches multiple assets. Search for these assets and update them with the correct unique IP Address if needed.

Manage Assets

If an asset has been created manually or through Auto Discovery, but the inventory service was **not** installed on the asset at that time, the **Update Asset** option will display after an Auto Inventory.

1. If the IP Address matches an eTrust VM managed asset IP Address, an **Update Asset** link will be displayed.
2. To enable inventory service communication with that asset, select **Update Asset**.
3. The inventoried technologies will be added to the asset profile at that time.

Create Assets

The Auto Inventory list displays IP addresses that have the eTrust VM Inventory Service installed. To accept the inventory service information and create an asset, select "Create Asset."

1. If no match of IP Addresses is found, a **Create Asset** link will be available.
2. Click **Create Asset** to create the new asset.
3. After clicking **Create Asset**, the inventory service becomes **Enabled** for that asset, to continue communication with eTrust VM.
4. When the asset is created, an **AssetID** is generated by eTrust VM.
5. The **AssetID** is then stored in the service configuration file for each desktop.
6. Subsequent eTrust VM Service requests will then match the **AssetID** of the asset with AssetID in eTrust VM asset table. The match will no longer be performed on the IP Address.

Select **Delete** if the inventory service has been removed and the asset's information no longer needs to display on this list.

Dynamic IP Addresses

The eTrust VM Service may be installed on all desktops in order to match the AssetID of the configuration file with the AssetID of a managed asset. Then, Service communication must be **Enabled** from the Auto Inventory list in order for the service commands to send specific data to eTrust VM, such as the technologies on that IP Address.

This setting is especially important when using DCHP. Auto Discovery matches ONLY on the IP Address. If the IP Address is dynamic, eTrust VM Services performed at later dates may not find a match. However, if the Service is enabled, the match is then performed on the AssetID, not the IP Address, as indicated above.

Additional notes:

- IP Addresses need not be unique.
- If multiple matching IPs are found, two rows are returned. User may create two assets with the same IP, but it will have different AssetIDs.
- If three or more are found, a third asset will be created.
- If an IP Address is returned as 0.0.0.0, the service found multiple network cards and was unable to determine which was active.

ASSET MANAGEMENT

Assets (also known as asset profiles) are a type of inventory of technologies of the IT environment. Asset profiles track vulnerabilities affecting technologies, assets, or common configurations. Assets can be defined for either a specific asset (the production Web server) or for a common configuration (a Sun database server w/Oracle).

ASSET INFORMATION

The following fields will define an asset. All fields are **not** mandatory. See Asset Creation for details.

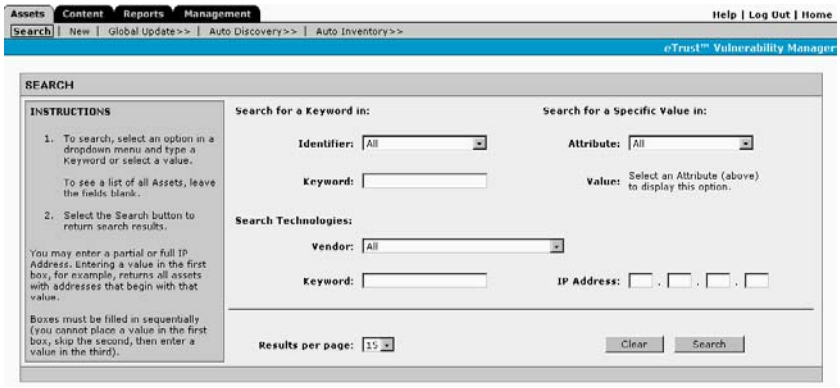
- Asset Name –unique across an eTrust VM
- Risk–High, Medium and Low with Low being the default selection
- Asset Function –functions include:
  - Mail Server
  - Remote Access Server
  - Database/File/Application Server
  - Security Server/Device
  - Web Server
  - Workstation
- AssetID, generated by eTrust VM
- Asset TagID, user input
- Location- such as building, department, floor, etc
- Model – the model of asset, such as 168D90, etc
- Manufacturer – the manufacturer of the asset, such as Dell, Cisco, etc
- Description - brief description of the asset
- Technology Associations- technologies on that asset
- Patch Associations –patches that have been applied to this assets technologies
- Qualified Domain Name – optional
- Host Name – optional
- IP Address- optional
- Subnet Mask – optional
- MAC Address – optional
- Created By– this is system generated

ASSET SEARCH

The standard search function is used in order to find an asset for viewing, maintaining or performing an audit assessment on that asset. Users may search assets by Key Word and/or by specific field values.

To search for an asset:

1. **Search for keywords** within the text field selected from the dropdown menu.
2. Select a **defined field**, then select **a specific value** to search for in that field.
3. Search for a **technology** by selecting a **Vendor** then searching for a **keyword**.
4. Indicate the **number of results per page** to be displayed (15-90, in increments of 15).
5. Broaden search by leaving field values as **All** and keyword fields blank.

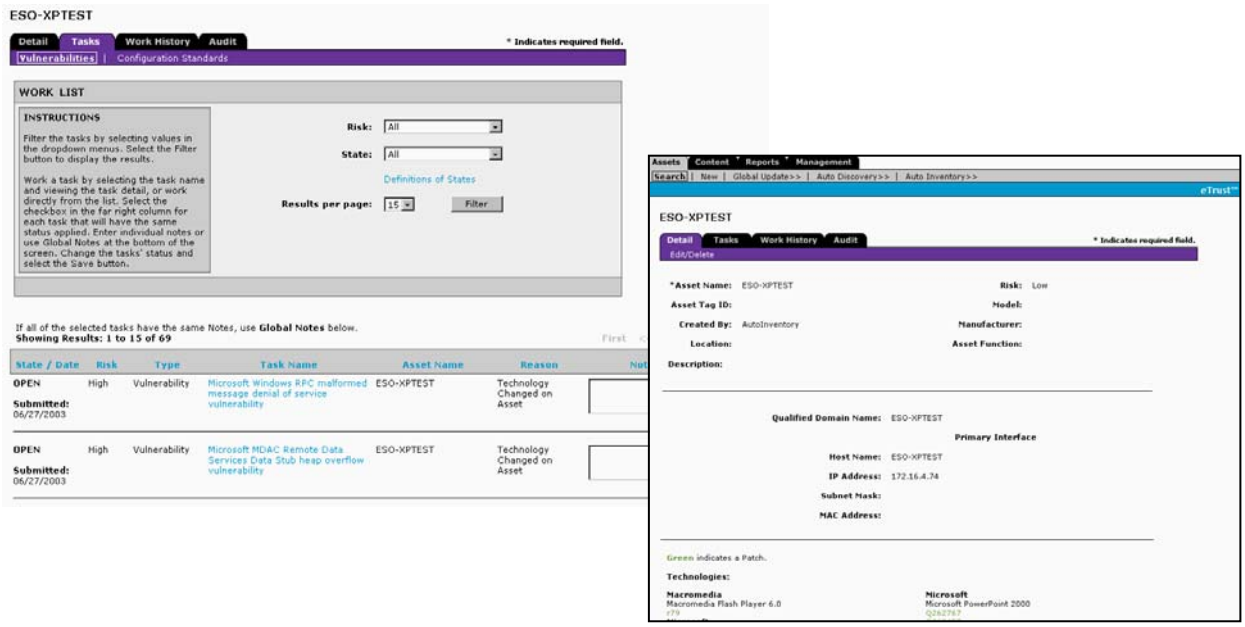


Keyword Search Logic

Type keyword(s) to find names and/or descriptions that START with the full or partial keyword(s).
(e.g. HP-UX, acrobat, windows2000)
To search names/descriptions that CONTAIN the keyword, type and asterisk(*) before the keyword(s).
(ex: *HP, *acrobat, *web server)

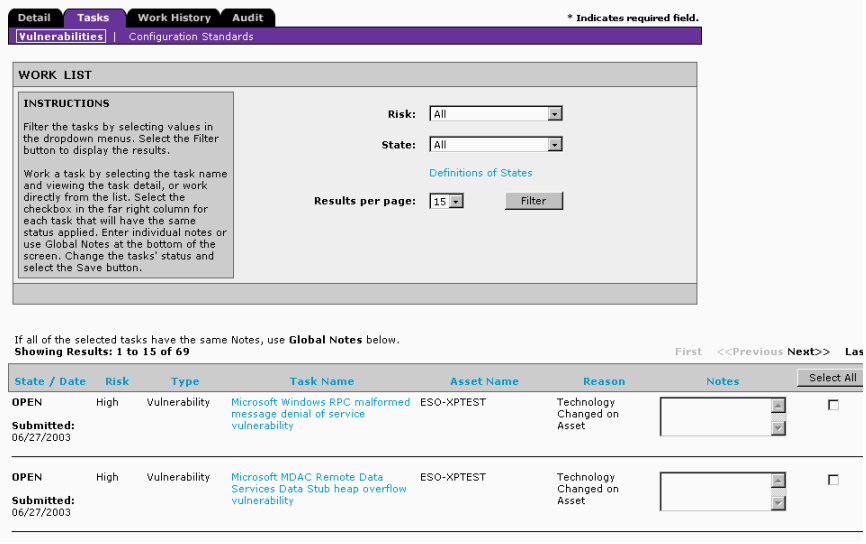
ASSET DETAIL

After performing an asset search, the results are displayed below the search form. From these search results, the asset detail can be displayed by clicking on the asset name.



TASKS FOR EACH ASSET

To display tasks for each asset, click the **Tasks** tab from the asset detail screen. A worklist is displayed that contains all tasks associated to that asset. The tasks can be filtered by **Risk** level, and by the **State** of the task.



ASSET CREATION

There are three methods by which an asset can be created in eTrust VM.

1. The user can utilize the Auto Discovery feature.
2. The user can utilize the Auto Inventory feature.
3. The user can create the asset manually.

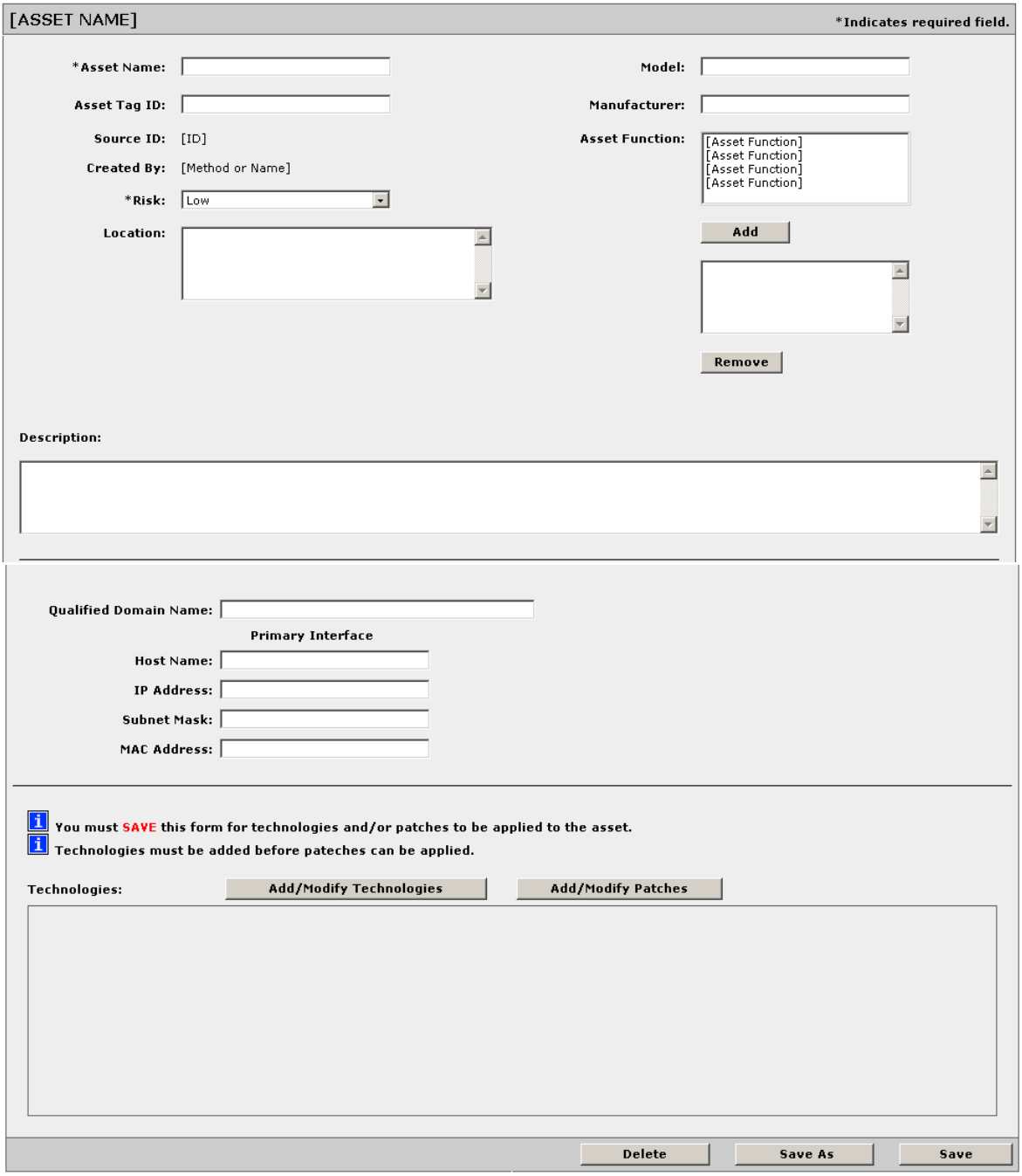
For Manual Asset Creation:
Required fields are designated by an asterisk on the create screen, shown on the next page.

1. Click **Assets>New** from tab menu to display the new asset form.
2. Input data in all required fields and optional fields, if applicable.
3. Enter the **Asset name**, which must be unique for eTrust VM.
4. AssetID, generated by eTrust VM.
5. 'Created By' field, generated by eTrust VM.
6. **Select the risk level** of this asset, High, Medium or Low.
7. Enter the **location** of this asset (ex. building, department, floor, etc).
8. Enter the **Model** of this asset (ex. 1633d).
9. Enter the **Manufacturer** of this asset (ex. Dell).
10. Select the **Function** of this asset.
11. Click '**Add'**. The functions are copied to the field below.
12. To remove a function, select the function and click '**Remove'**.
13. Add a **description** of this asset.
14. Specify the **Qualified Domain Name** of this asset.
15. Enter the **Host Name, IP Address, Subnet Mask and MAC Address** of this asset.
16. Add **associated technologies** to this asset. See the Associated Technologies section. This step MUST precede the Add Patches step.
17. Add **associated patches** to this asset. See the Associated Patches section.
18. Click '**Save'** to create the Asset.

Assets may be only be deleted manually, from the Asset Profile.

See the ***Asset Create*** form on the following page.

ASSET CREATE FORM

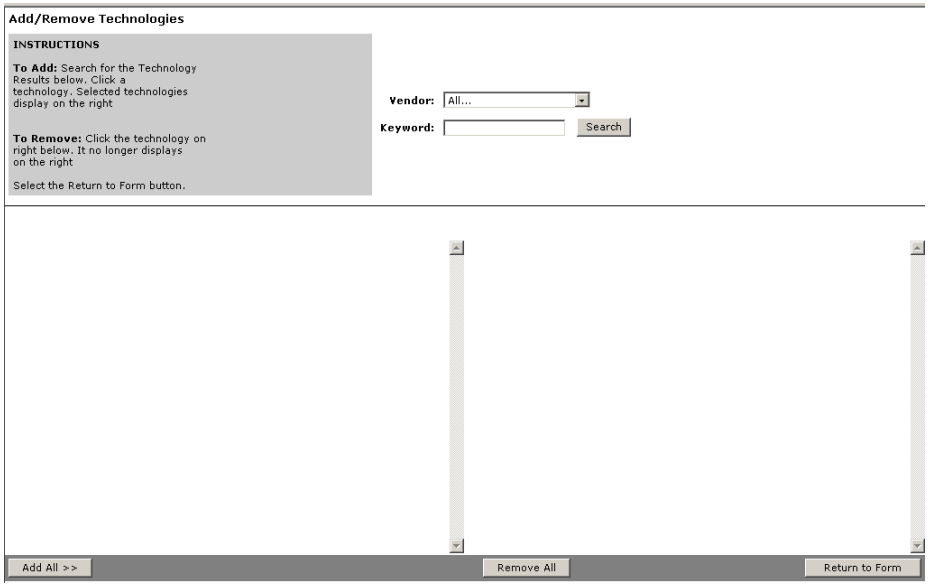


ASSOCIATED TECHNOLOGIES

Users are able to add or remove technologies to Assets within eTrust VM. When the 'Associated Technologies' link is clicked, the screen below is displayed. If any technologies have been previously associated, they will be displayed in the right hand column. In the example below, a search was performed that displayed the results in the left hand column. No previous technologies were associated.

To Update Technologies

1. Click **Add/Remove Technologies** from the Asset Profile/Create screen.
2. Search for technologies to associate.
3. Select the technology **vendor**.
4. Select a **keyword** for that vendor, such as 'Windows'.
   Or, Select **All** vendors and enter a keyword to be searched.
5. Click **Search**.
6. Search results are displayed in the left side column of the display below.
7. Select the specific technology to associate by clicking on it. It will appear in the right hand column.
   Or, click **Add All** to add all listed technologies to the right hand column.
8. The technology will appear in the right hand column.
9. To remove a technology, select the technology from the right side column.
   Or click **Remove All** to select all technologies. They will appear in right hand column for removal.
10. When all selections are complete, click **Return to Form**. This returns the user to the previous form.
11. Continue with the previous form. The user must **Save** the form in order for the technologies to be associated.



ASSOCIATED PATCHES

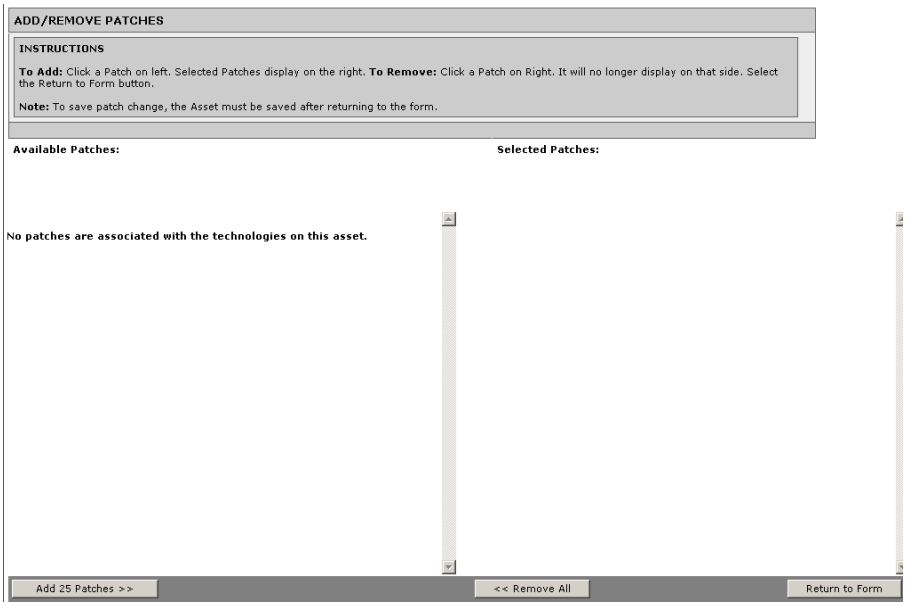
A patch is a fix that has been determined for a specific technology. The Add/Remove Patches screen allows the user to apply one or more patches associated to a technology. The system will then list all assets that can be updated with the patch information, and the associated vulnerability work items that may be statused as a result of applying the patch. When the user accepts the application of a patch, the asset will be updated and the work items statused. This feature may be implemented from a global perspective utilizing the Global Update functionality, or on an individual asset basis, through creation or modification of an asset.

To Add Patches to an Assets Technologies:

1. After associating technologies to the asset, the **Add/Remove Patches** link becomes available on the form.
2. Click **Add/Remove Patches** link to display the list of patches associated to those technologies.
3. The user will **select the patches to be applied or click Add All** to select all listed patches.
4. Click **Return to Form** to apply the patches.
5. Click **Save** to complete the asset creation.
6. The results of applying the patch will display a report of the vulnerabilities that were affected, along with the status.

Patches may also be removed, but only for associated vulnerabilities with a status of Implemented. If the patch is removed then the application will remove the Implemented status, 'Re-Open' the task " and remove the patch name from the notes field of each affected task.

See the Asset Create or Asset Update Sections. See also Global Updates/Patches, for specific step-by-step instructions.



ASSET UPDATE

eTrust VM provides the ability to **Edit** assets when changes are required and to **Delete** assets that are no longer needed. eTrust VM also provides the ability to create a new asset from an existing asset with the "save as" function. Assets can be updated manually or via the Auto Inventory process. Auto Inventory provides the functionality to update the technologies.

To Edit or Delete an existing Asset:

1. After searching for a specific asset, click the **Asset Name** to display the asset.
2. The Asset Profile information will display, with the **Details** tab displayed as the default.
3. Select the **Edit/Delete option**, under the **Details** tab.
4. The Asset is displayed in **Modify mode**.
5. Make the necessary modifications to the appropriate fields.
6. To Add/Remove Technologies, see the Associated Technologies section.
7. To Add/Remove Patches, see the Update Patches section.
8. After all fields are complete, select one of these three options:

   Save--Modify assets and save the changes
   Delete--Completely delete the Asset
   Save As--To save the Asset under a different name.

If the following values are changed, the asset impact analysis will be launched.

Risk Level
Asset Function
Adding or Removing Technologies
Adding or Removing Patches

ASSET DELETE

An asset may only be deleted manually, from the Asset Profile screen.

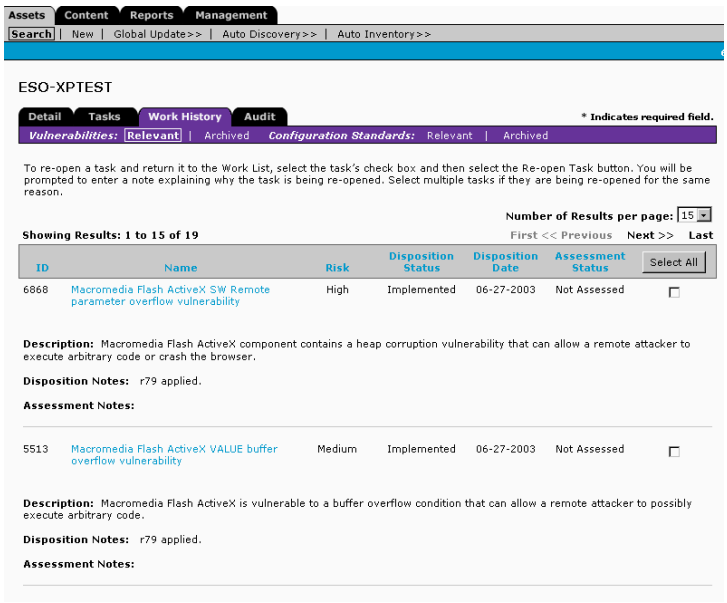
1. **Search for the Asset** from the Asset> Search function.
2. Click **delete**.

See Asset Update for more information.

WORK HISTORY OF AN ASSET

The Work History is a list of all statused work items such as vulnerability tasks and, if applicable, the configuration standard tasks for each asset. Users have the ability to print the Work History Relevant and Archived reports.

From the Asset Detail screen, the Work History can be displayed for that asset. Click the **Work History** tab.



Relevant Work Items

When a task has been completed, it is removed from the Work List and becomes part of the asset's Work History, Relevant Items. From the Work History Relevant screen a task can be re-opened. If re-opened, the item will no longer be part of the Work History Relevant of the asset, but it will be considered part of the Work History Archived. There, opened item statused on the work list will be **New** with an attribute of **Re-Opened**.

Only Relevant Work Items can be reopened. To re-open a task and return it to the Work List:

1. Select the task's check box and then select the **Re-open Task button**.
2. You will be prompted to enter a note explaining why the task is being re-opened.
3. Select multiple tasks if they are being re-opened for the same reason.

Archived Work Items

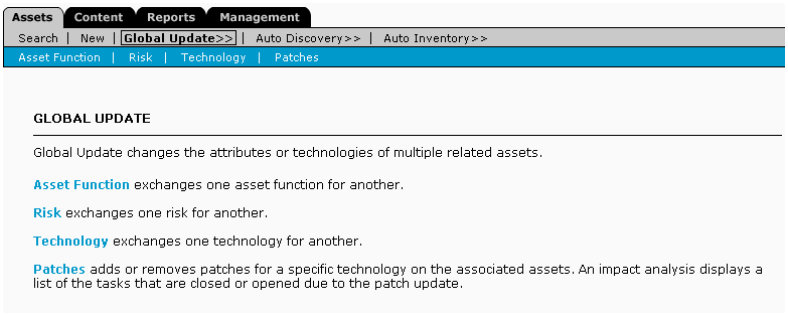
Items are archived based on the results of the asset impact analysis when there has been a change on the asset or a change in a Vulnerability or Configuration Standard, which makes the task no longer applicable. These work items become part of the Asset's Work History, Archived Items.

GLOBAL UPDATE OF ASSETS

The Global Update function provides the ability to update specific fields or attributes of multiple assets. The following asset attributes can be globally changed:

1. **Asset Function**--update the function on multiple assets
2. **Asset Risk Level**--update the risk on multiple similar assets, High, Medium or Low
3. **Technology**--update a technology associated to multiple assets
4. **Patch**--update the patches that have or have not been applied to multiple assets

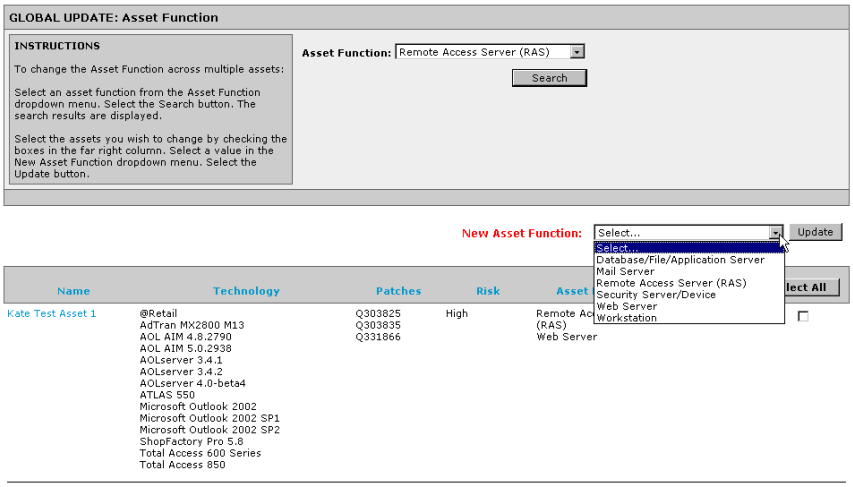
In order to update an asset, a search is first performed for assets that include one of the attributes listed above. Only one attribute may be globally updated at a time.



UPDATE THE ASSET FUNCTION

Upon update of the Asset Function, the Impact Analysis will be launched. Check the work list for additional tasks. To change the Asset Function across multiple assets:

1. **Select an asset function** from the dropdown menu.
2. Click **Search**. The search results are displayed.
3. **Select the New Asset Function** from the dropdown menu.
4. **Select the assets** you wish to change to the new function by checking the boxes in the far right column. Or, select all by clicking the **Select All** button.
5. Click **Update** to save the changes.

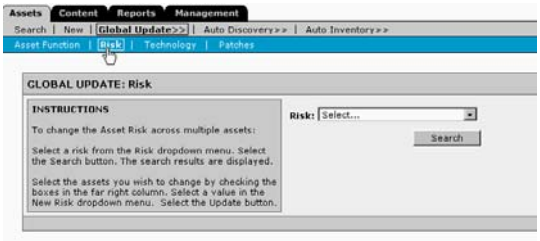


UPDATE THE ASSET RISK LEVEL

To change the Asset Risk Level across multiple assets:

1. Select the specific **Risk Level** to change from the dropdown menu.
2. Click **Search**. The search results are displayed.
3. Select the **New Risk Level** from the dropdown menu.
4. **Select the assets** you wish to change to the new risk level by checking the boxes in the far right column. Or, select all by clicking the **Select All** button.
5. Click **Update** to save the changes.

Upon update of the Asset Risk Level, the Impact Analysis is launched. Check the work list for additional tasks.

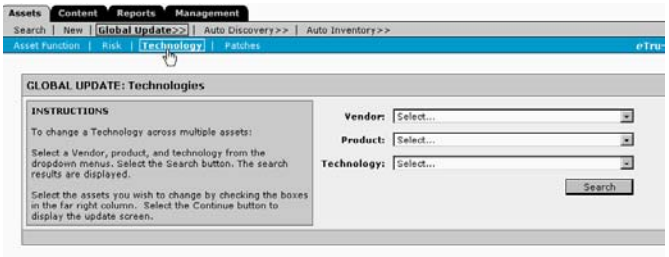


UPDATE THE TECHNOLOGY

To change the Technology across multiple assets:

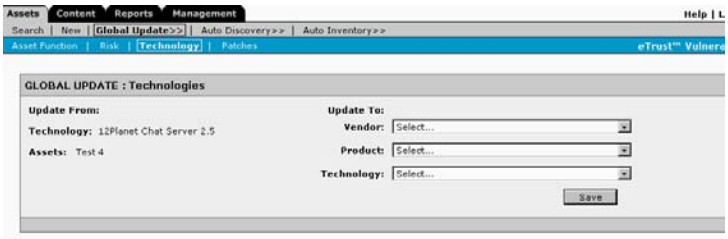
1. **Select the Vendor** from the dropdown menu.
2. **Select the Vendor's Product** from the dropdown menu.
3. **Select the specific Technology** for that Product from the dropdown menu.
4. Click **Search**. The search results are displayed.
5. **Select the assets** you wish to change to the new Technology by checking the boxes in the far right column. Or, select all by clicking the **Select All** button.
6. Click **Continue** to display the update screen.

Upon update of the Technologies, the Impact Analysis will be launched. Check the work list for additional tasks.



To change the Technology for the **Assets to Update** listed:

1. **Select the Vendor** from the dropdown menu.
2. **Select the Vendor's Product** from the dropdown menu.
3. **Select the specific Technology** for that Product from the dropdown menu.
4. Click **Save** to update the technology for all assets listed.



UPDATE THE PATCH

Add A Patch

To Add a Patch(es) to a Technology, search for Patches associated to a specific technology:

1. **Select the Vendor** from the dropdown menu.
2. **Select the Vendor Product** from the dropdown menu.
3. **Select the specific Technology** for that Product from the dropdown menu.
4. Click **Search**. All Patches associated to that technology are displayed.
5. Click a patch on the left, under **Available Patches**, to apply, or select **Add All**.
6. The patch is displayed in the right column, **Selected Patches to Apply**.
7. Click **Add to Assets** to continue.

The results display a list of vulnerability tasks that will be implemented if the Patch is applied.

Apply the Patch

To Add the Listed Patches to Assets and Associated Tasks:

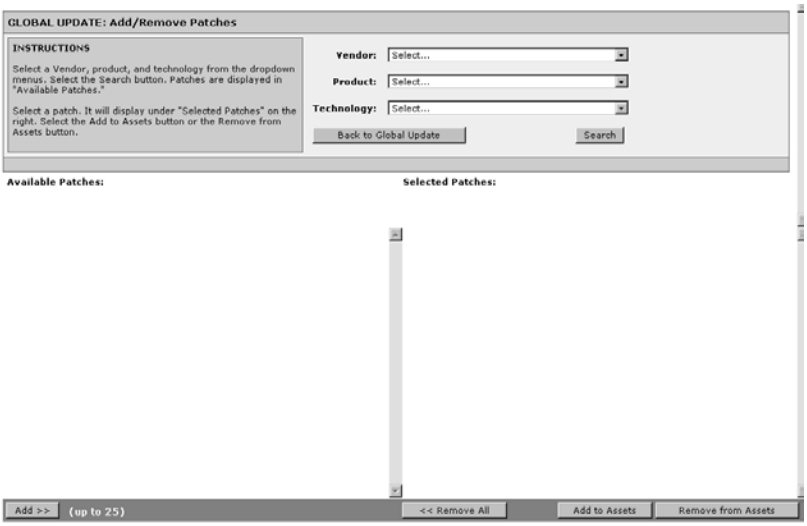
1. **Select the Asset/Task(s) to apply** each Patch to by checking the box in the far right column.
2. Click **Select All** to apply the Patch to all Assets/Tasks listed.
3. **Repeat** above steps for each Patch listed.
4. Click **Apply** at the bottom of the screen to commit the changes.
5. Click **Cancel** at the bottom of the screen to ignore.
6. Click **Print** at the bottom of the screen to print this page.

Remove Patch From a Technology

To Remove Patch(es) from a Technology, search for Patches associated to a specific technology:

1. **Select the Vendor** from the dropdown menu.
2. **Select the Vendor Product** from the dropdown menu.
3. **Select the specific Technology** for that Product from the dropdown menu.
4. Click **Search**. All Patches associated to that technology are displayed.
5. Click a patch on the right, under **Selected Patches to Apply** or select **Remove All**.
6. Selected patches are highlighted.
7. Click **Remove From Assets** to continue.

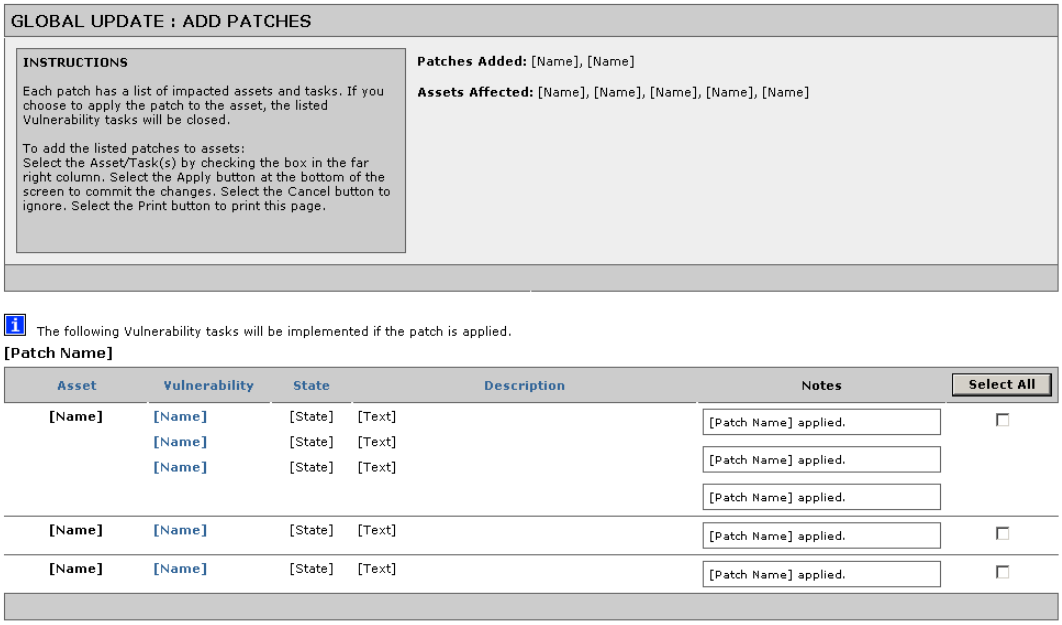
The results display a list of vulnerability tasks that will be implemented if the Patch is applied.



Remove Patch from an Asset

To Remove the Listed Patches from Assets and Associated Tasks:

1. **Select the Asset/Task(s)** from which **to remove** the Patch by checking the box in the far right column.
2. Click **Select All** to remove the Patch from all Assets/Tasks listed.
3. **Repeat** above steps for each Patch listed.
4. Click **Apply** at the bottom of the screen to commit the changes.
5. Click **Cancel** at the bottom of the screen to ignore.
6. Click **Print** at the bottom of the screen to print this page.



ASSET IMPACT ANALYSIS

Events will occur within eTrust VM that will cause the system to launch the Asset Impact Analysis. The analysis determines the impact on an asset's tasks based on certain data modifications to an asset, the addition or deletion of vulnerabilities or configuration standards, or a change in eTrust VM settings. The results for the analysis can be any of the following:

Adding tasks to the Work List.

Tasks may be added when the following occurs:

- A technology is added to an asset, vulnerability or a configuration standard.
- Risk setting is changed to include additional task risk levels.
- Asset Function is changed on an asset or a configuration standard.
- Risk is changed on an asset or a configuration standard.

Removing "open" tasks from the Work List.

Tasks may be removed when the following occurs:

- A technology is removed from an asset, vulnerability or a configuration standard.
- Risk setting is changed to exclude lower risk items.
- Asset Function is changed on an asset or a configuration standard.
- Risk is changed on an asset or a configuration standard.

Archiving tasks that have been "completed".

Completed Tasks will be archived when the following occurs:

- The task no longer applies to the asset because of a modification to the asset, vulnerability or configurations standard.

Any vulnerability or configuration standard task that is "open" on the work list that no longer applies due to the data change will be deleted from the work list regardless of its "locked" status.

WORK LIST

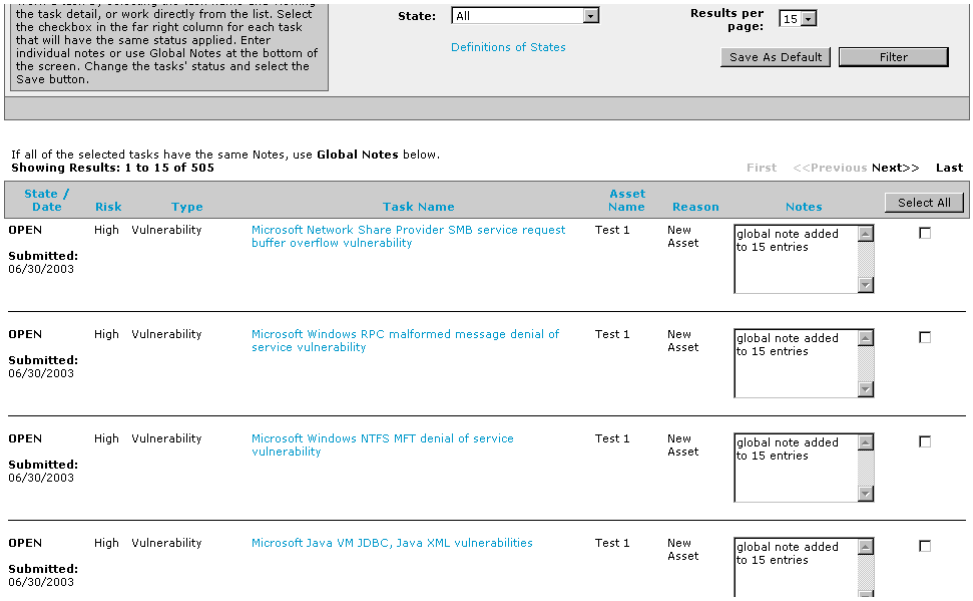
The Work List is a listing of all vulnerability and configuration standard tasks that should be addressed in some way by the system administrators. The Work List will be displayed on the homepage, upon login, which will list all tasks, sorted by risk (High, Medium, Low). eTrust VM Configuration settings determine if configuration standards tasks are displayed and also which risk levels to display.

Functionality of the Work List includes:

- The ability to change the 'Status' of a single task or multiple tasks
- The ability to filter the work list
- The ability to add individual notes and global notes to multiple tasks
- A Print option to generate the work list report
- The ability to export the list via a CSV file.

The Work List is a group (shared) list. Any user can view the work list, but tasks opened by other users cannot be updated. When an individual takes ownership of a work item, that item is locked.

To display the entire worklist from the Home Page, leave filter criteria as **All** and click **Filter**. A work list is shown below.



STATE OF A TASK

The **State** of a Task indicates to whom that task belongs.

1. Open, belongs to no user at this time.
2. Personal, belongs to the logged-in user.
3. Locked, belongs to another user.

FILTER THE WORK LIST

The work list can be filtered and each user also has the option to set a default filter criteria for their own view of the Current Work List.
To Filter:

1. Filter the task list by selecting values from the dropdown menus.
   The Current Work List has the following search/filter criteria:
   - Task Type (All, Vulnerabilities, or Configuration Standards)
   - Risk (High, Medium and Low)
   - State (All, Open, Personal, or Locked]
   - Asset Name
   - Asset Function.
2. Click **Filter** to refresh the work list.
3. Click **Save as Default** to save this filter criteria.
4. Click the **Home** link at the top of the page to reload the default filter, which is 'All'.

WORK LIST STATUSES

The **Status** of a Task refers to the actual work that has or will be done on the task itself.

The work list will display all open tasks that have not had a status assigned yet. After a task has been worked, it is assigned a status and removed from the current task list, becoming an item in the asset's work history.
The work list statuses are:

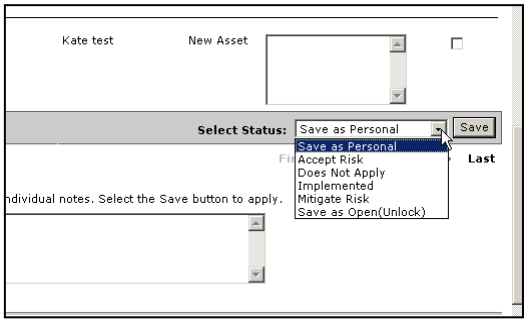
- **Save as Personal** – This status assumes the user is taking ownership, or responsibility for reviewing, taking action on, reporting status and/or completing the task. The state of the task will be **Personal** when the user who took ownership views the work list. For non-owners the state will be **Locked**.
- ****Accept Risk**- the user is accepting the risk associated with this task. This task is not being implemented.
- ****Does Not Apply**- this task does not apply to the specific asset, for reasons determined by the user.
- ****Implemented**- this task has been implemented and the recommended actions were performed.
- ****Mitigate Risk**--the user indicates they are mitigating this risk by taking another action.
- **Save as Open (unlock)**- Removes the task from the Work History and displays it back on the Work List.

****-**The above referenced statuses represent a 'Completed' task. Completing a task requires the user to assign a status for the item and save the action, removing the task from the work list.

STATUS THE TASKS

To modify the status of a task:

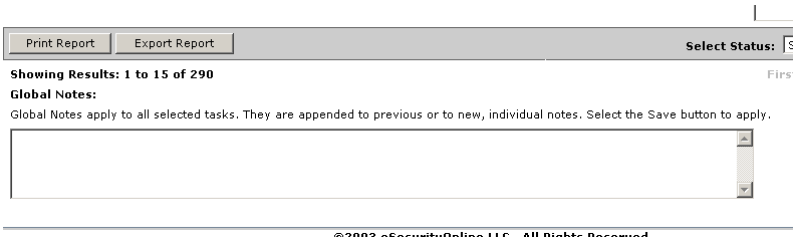
1. From the work list on the Home page, select the checkbox in the far right column for the specific task or for multiple tasks.
2. Change the task status using the dropdown menu at the bottom of the work list.
3. Add notes in the notes field for the selected task and click **Save** at the bottom of the work list.
4. To select the same status for all tasks in the entire work list, click the **Select All** button at the top of the work list.



GLOBAL NOTES

A global note may be added to multiple tasks or all tasks in the displayed work list.
To apply a global note:

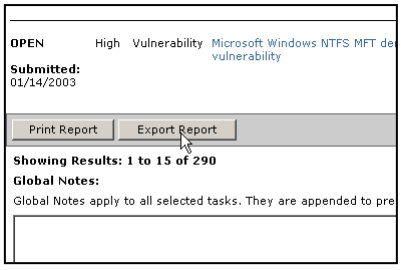
1. From the Work List on the Home page, select the checkbox in the far right column for each specific task. Or, to apply a global note to all tasks in the work list, click **Select All** at the top of the work list.
2. Type the note in the **Global Notes** field at the bottom of the page.
3. Click **Save** to apply.
4. The note is appended to all previous notes for the task(s) selected.



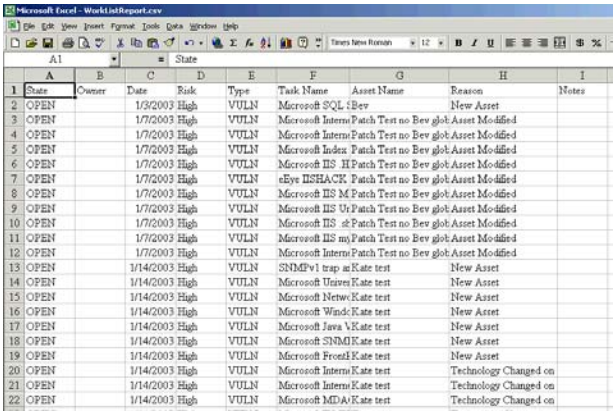
EXPORT THE WORK LIST

The work list can be exported into a CSV spreadsheet and displayed in Microsoft Excel.

Click the **Export Report** button at the bottom of the work list.



Below is an example of a work list report, imported as a CSV file.



CONTENT

The content or data housed in eTrust VM is located within the Content tab. Vulnerabilities and Configuration Standards can be searched and viewed. The user can also determine if Vulnerabilities or Configuration Standards affect any of eTrust VM managed assets.

After an asset is configured, installed and added to the system, Vulnerabilities and Configuration Standards that match the asset technologies will be applied to the asset. The content (Vulnerabilities and Configuration Sstandards) is evaluated and work list items are generated, if applicable.

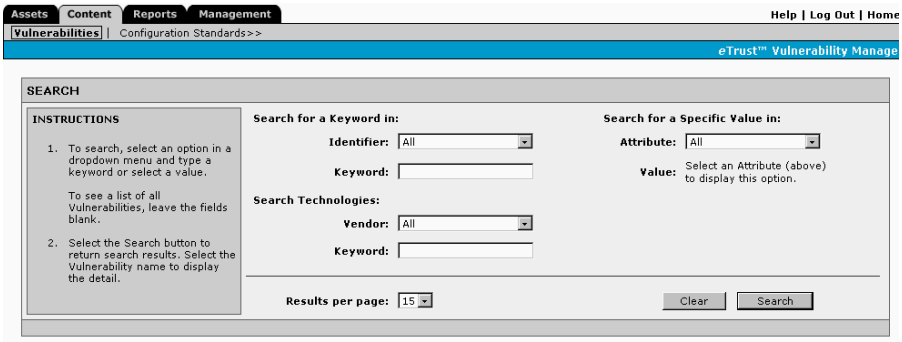
VULNERABILITIES

The Vulnerabilities component provides detailed information about Vulnerabilities that could affect your assets and the associated technologies. Tasks are generated and placed on the work list from Vulnerabilities that affect the assets and technologies inventoried in the eTrust VM.

Vulnerabilities Search

Users can search for Vulnerabilities based on keyword, category and/or technology.

1. Search for keywords within the text field selected from the dropdown menu.
2. Select a defined field, then select a specific value to search for in that field.
3. Search for a technology by selecting a Vendor, then searching for a keyword.
4. Indicate the number of results per page to be displayed (15-90, in increments of 15).
5. Broaden search by leaving field values as **All** and keyword fields blank.
6. Type a leading asterisk in the keyword search field to find all items containing that text.



Keyword Search Logic

Type keyword(s) to find names and/or descriptions that START with the full or partial keyword(s).
(e.g. AIX, Navigator, OSF1)
To search names/descriptions that CONTAIN the keyword, type and asterisk(*) before the keyword(s).
(e.g. *AIX, *navigator, *OSF1)

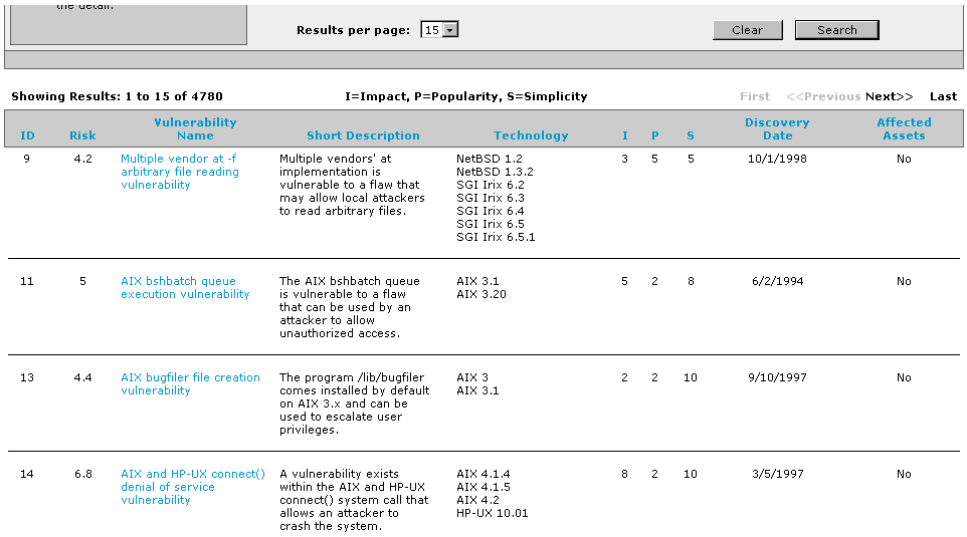
Vulnerability Search Results

The Vulnerability search results display all Vulnerabilities housed in the eTrust VM content, if 'All' was used in all fields of the search criteria. Information included in the Vulnerability list includes:

- Vulnerability ID
- Risk rating
- Vulnerability Name
- Short description
- Technologies associated
- Impact, Popularity and Simplicity rating
- Discovery Date
- Assets that are Affected

Most search result columns allow a sort on that column by clicking the header. The column header will be sorted in ascending order. If the user clicks on the same column, the sort order is reversed.

1. Select a **Name** to display the Vulnerability detail.
2. If assets are affected by the vulnerability, a link is provided. Click **Yes** to display 'Affected Assets'.



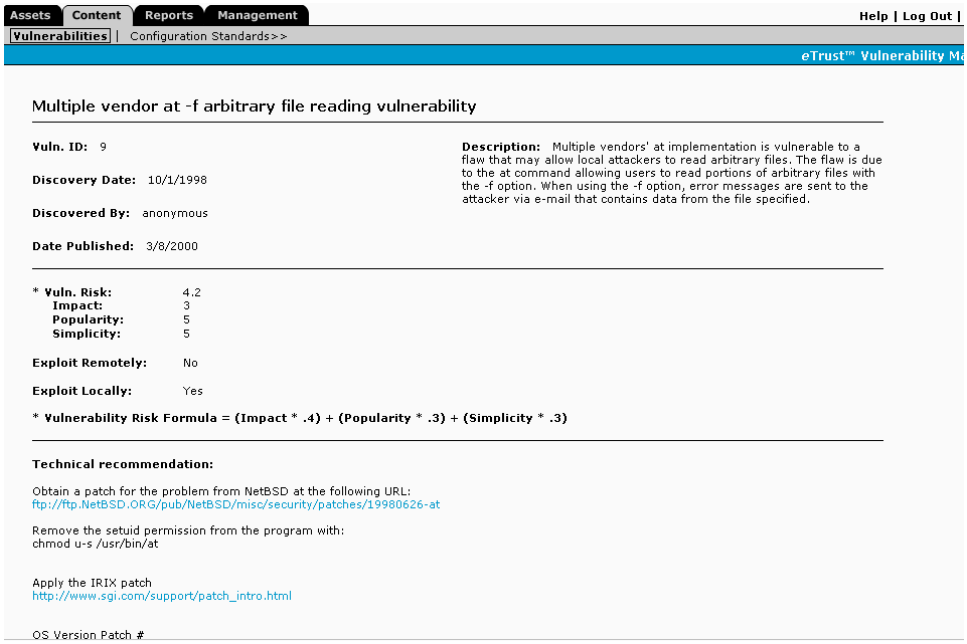
Results per page: 15 Clear Search

Showing Results: 1 to 15 of 4780 I=Impact, P=Popularity, S=Simplicity First <<Previous Next>> Last

ID	Risk	Vulnerability Name	Short Description	Technology	I	P	S	Discovery Date	Affected Assets
9	4.2	Multiple vendor at -f arbitrary file reading vulnerability	Multiple vendors' at implementation is vulnerable to a flaw that may allow local attackers to read arbitrary files.	NetBSD 1.2 NetBSD 1.3.2 SGI Irix 6.2 SGI Irix 6.3 SGI Irix 6.4 SGI Irix 6.5 SGI Irix 6.5.1	3	5	5	10/1/1998	No
11	5	AIX bshbatch queue execution vulnerability	The AIX bshbatch queue is vulnerable to a flaw that can be used by an attacker to allow unauthorized access.	AIX 3.1 AIX 3.20	5	2	8	6/2/1994	No
13	4.4	AIX bugfiler file creation vulnerability	The program /lib/bugfiler comes installed by default on AIX 3.x and can be used to escalate user privileges.	AIX 3 AIX 3.1	2	2	10	9/10/1997	No
14	6.8	AIX and HP-UX connect() denial of service vulnerability	A vulnerability exists within the AIX and HP-UX connect() system call that allows an attacker to crash the system.	AIX 4.1.4 AIX 4.1.5 AIX 4.2 HP-UX 10.01	8	2	10	3/5/1997	No

Vulnerability Detail

The Vulnerability detail is a view-only display of the Vulnerability.



Assets | Content | Reports | Management — Help | Log Out |

Vulnerabilities | Configuration Standards>>

eTrust™ Vulnerability M

Multiple vendor at -f arbitrary file reading vulnerability

Vuln. ID: 9

Discovery Date: 10/1/1998

Discovered By: anonymous

Date Published: 3/8/2000

Description: Multiple vendors' at implementation is vulnerable to a flaw that may allow local attackers to read arbitrary files. The flaw is due to the at command allowing users to read portions of arbitrary files with the -f option. When using the -f option, error messages are sent to the attacker via e-mail that contains data from the file specified.

* **Vuln. Risk:** 4.2
Impact: 3
Popularity: 5
Simplicity: 5

Exploit Remotely: No

Exploit Locally: Yes

* **Vulnerability Risk Formula = (Impact * .4) + (Popularity * .3) + (Simplicity * .3)**

Technical recommendation:

Obtain a patch for the problem from NetBSD at the following URL:
ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/patches/19980626-at

Remove the setuid permission from the program with:
chmod u-s /usr/bin/at

Apply the IRIX patch
http://www.sgi.com/support/patch_intro.html

OS Version Patch #

CONFIGURATION STANDARDS

Users have the ability to view the general Configuration Standard information and to create a build plan for assets from this content.

Configuration Standards Search

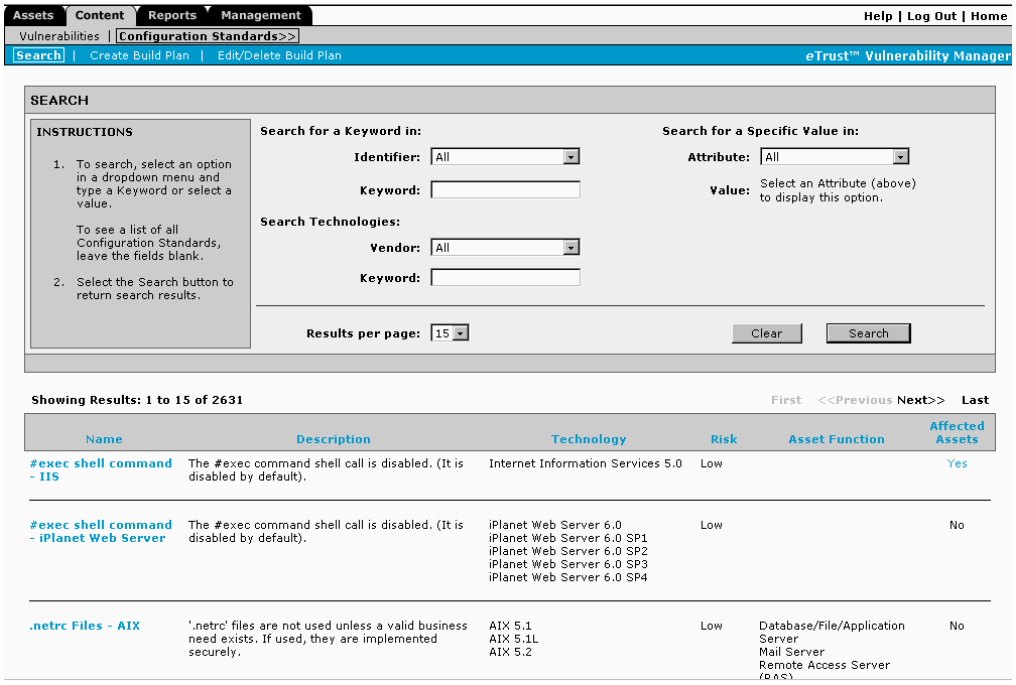
Users can search for Configuration Standards based on keyword, category, and/or technology.

1. Search for keywords within the text field selected from the dropdown menu.
2. Select a defined field, then select a specific value to search for in that field.
3. Search for a technology by selecting a Vendor, then searching for a keyword.
4. Indicate the number of results per page to be displayed (15-90, in increments of 15).
5. Broaden search by leaving field values as **All** and keyword fields blank.
6. Type a leading asterisk in the keyword search field to find all items containing that text.

Configuration Standards Search Results

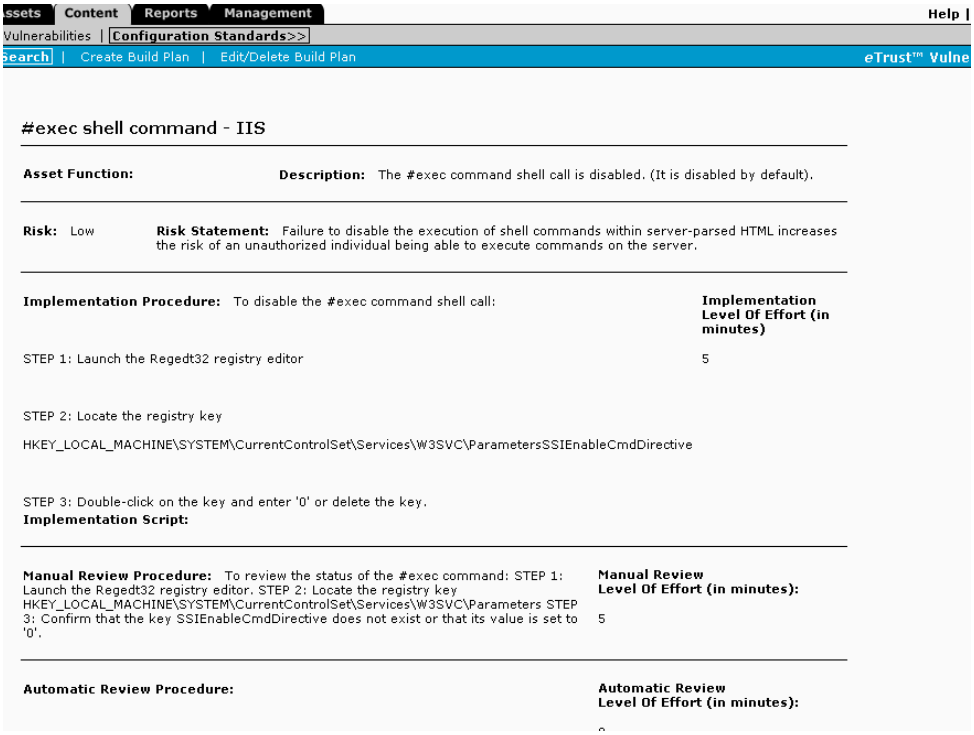
Most search result columns allow a sort on that column by clicking the header. The column header will be sorted in ascending order. If the user clicks on the same column, the sort order is reversed.

1. Select a Name to display the Configuration Standard detail.
2. If appliance managed assets are affected by the Vulnerability, a link is provided. Click **Yes** to display Affected Assets.



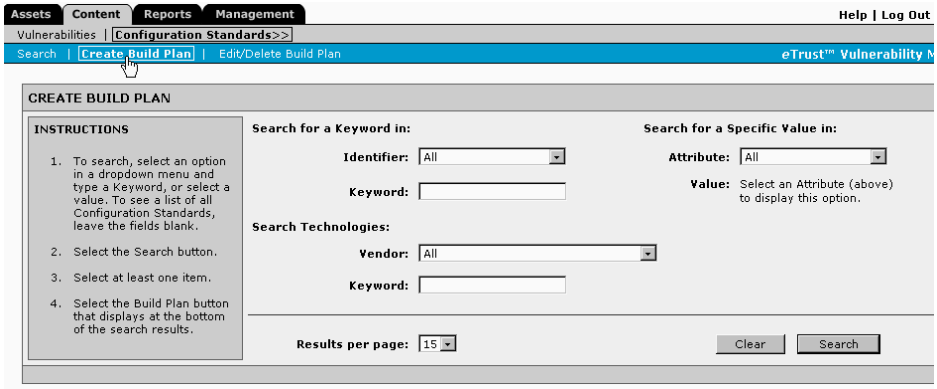
Configuration Standard Detail

The Configuration Standard detail is a view only display of the configuration standard.



Configuration Standard Build Plan

eTrust VM provides the ability to create a "build plan" of Configuration Standards that are required to configure a new asset based on Asset function and Technology. The Build Plan is intended to aid in setting up and physically configuring a new asset.

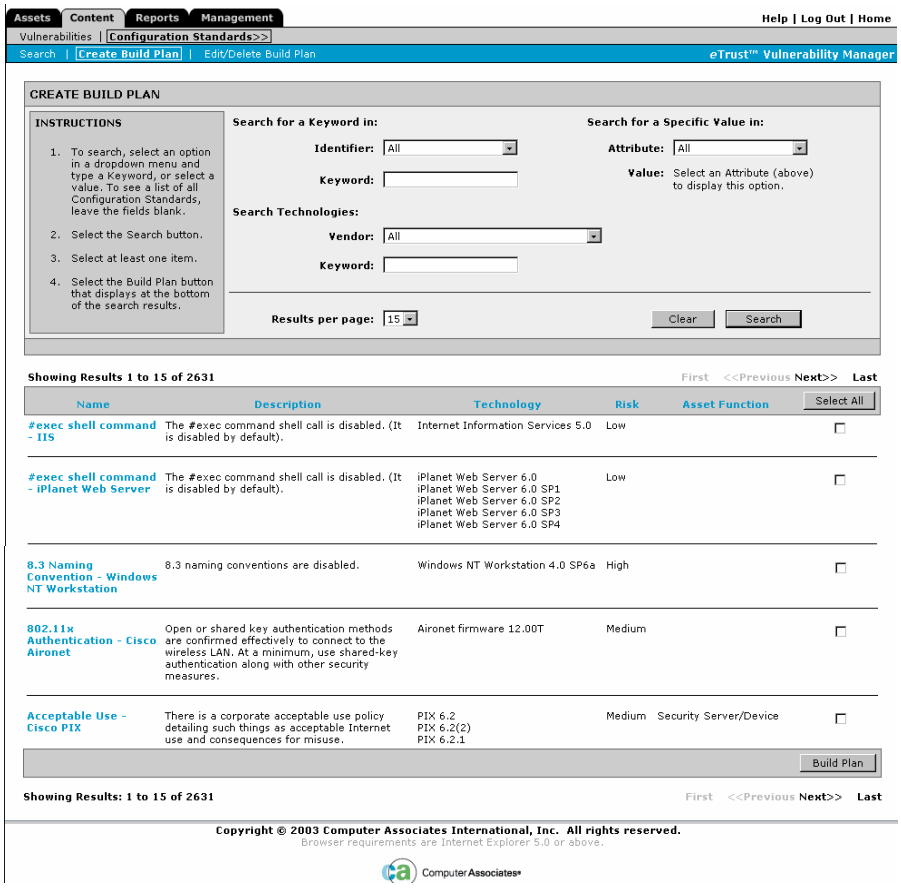


- The Build Plan consists of at least one Configuration Standard or a grouping of Configuration Standards selected by the user.
- Build Plans can be modified and deleted.
- An existing Build Plan may be used as a basis to create a new one ("Save As" function).
- The Build Plan name must be unique.

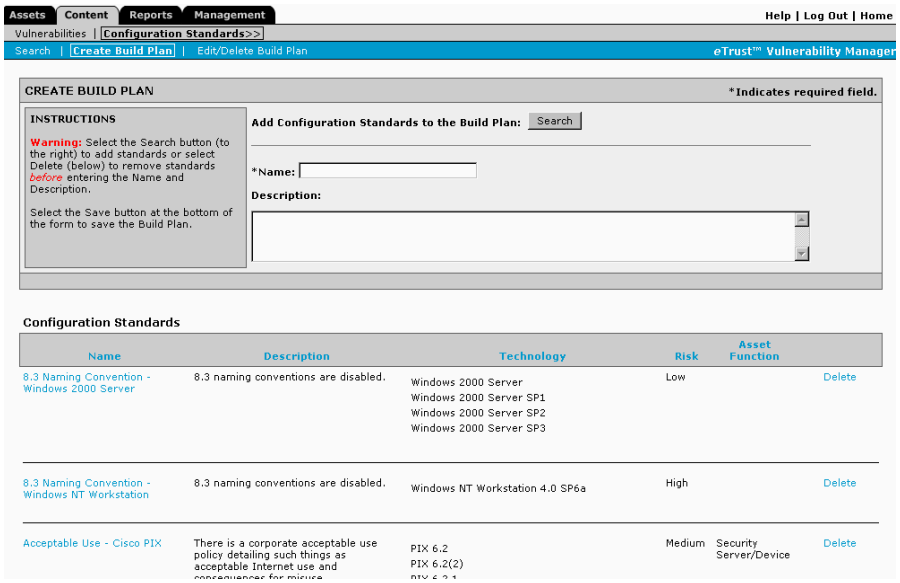
Create the Build Plan

To create a Build Plan, search for configuration standards.

1. Select **All** or narrow the search by filtering for Configuration Standards related to the asset.
2. Select the configuration standard(s) to be used in the build plan by checking the box in the right column. Or, Select **All** to include all Configuration Standards displayed in the results.
3. Click **Build Plan** to continue.



4. Select a unique name for the Build Plan.



5. Include an optional description of the plan, if needed.
6. Click **Save** to save the Build Plan.

Note: If adding or deleting a configuration standard from this screen, it must be done BEFORE the name and description are input. If not, the previous unsaved name and description fields will be wiped out.

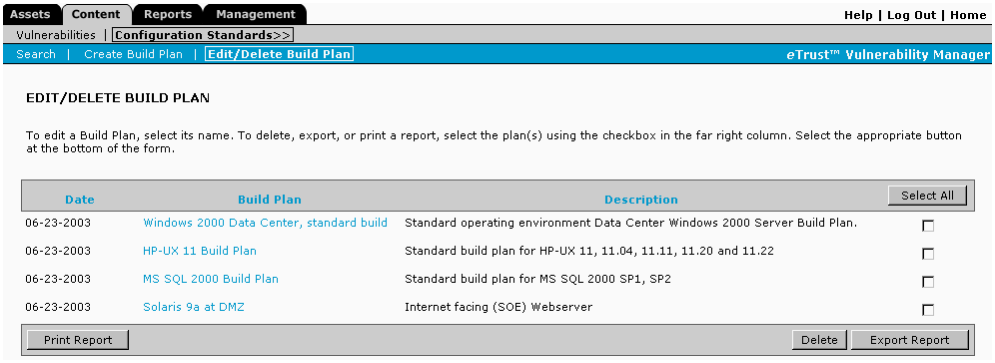
Edit or Delete the Build Plan

To edit a build plan:

1. **Select Content > Configuration Standards > Edit/Delete Build Plan**, from the tab menu.
2. All current Build Plans will be displayed.
3. **Click the build plan Name** to display the build plan.
4. Follow the **Create Build Plan** instructions above to edit.

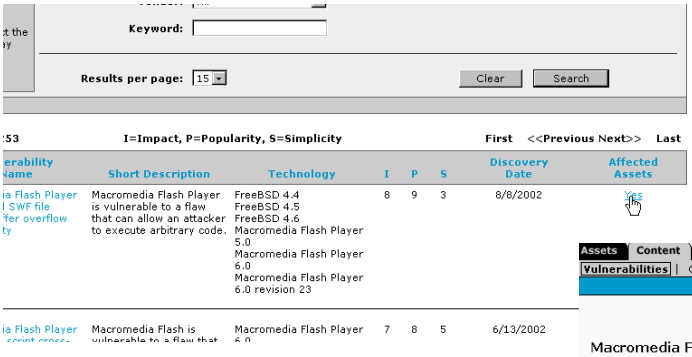
To delete a build plan:

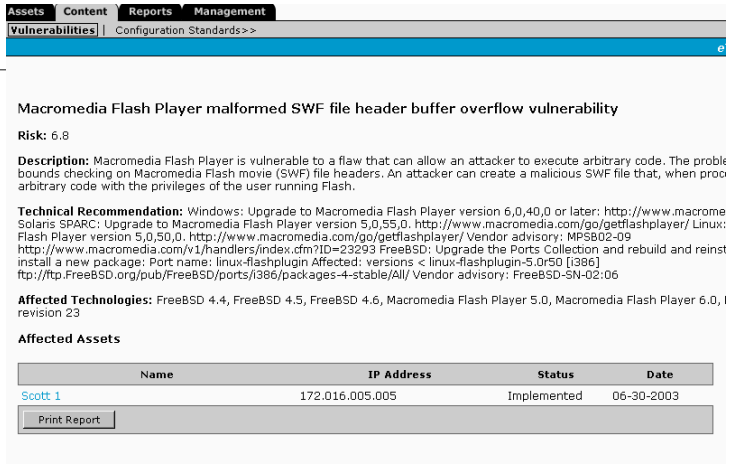
1. **Select Content > Configuration Standards > Edit/Delete Build Plan**, from the tab menu.
2. All current Build Plans will be displayed.
3. Select plans to delete by checking the box in the right column.
4. Or, **Select All** to delete all build plans.
5. Click **Delete** to save the changes.



AFFECTED ASSETS LIST

eTrust VM provides the ability to identify "affected assets" by producing a list of assets potentially impacted by a Vulnerability or Configuration Standard. The list will include those assets for which the fix may have already been applied or for which implementation of the fix is still outstanding. If there are associated work items for that asset, the status of that task will also be shown.





AUDIT FUNCTION

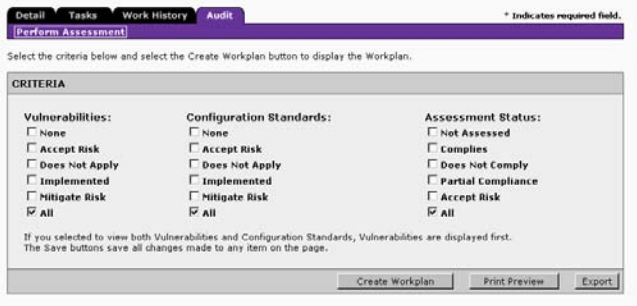
The Auditing function within eTrust VM provides organizations with the ability to measure compliance. Auditing enables proper accountability for security efforts and allows for a reconciliation of testing and fixing systems. The primary way of auditing and verifying the work of the system administrators is through the audit assessment.

AUDIT ASSESSMENT

Users can develop audit work plans based on closed tasks. The work plans list statused tasks and allow the user to enter an audit assessment status, as well as add notes. Available audit assessment statuses include *Not Assessed*, *Complies*, *Does Not Comply*, *Partially Complies* and *Accept Risk*.

Perform Audit Assessment

The Audit Assessment is on a per asset basis. The assessment is done on all the Vulnerabilities and Configuration Standards that have been assigned a work list status for an asset.



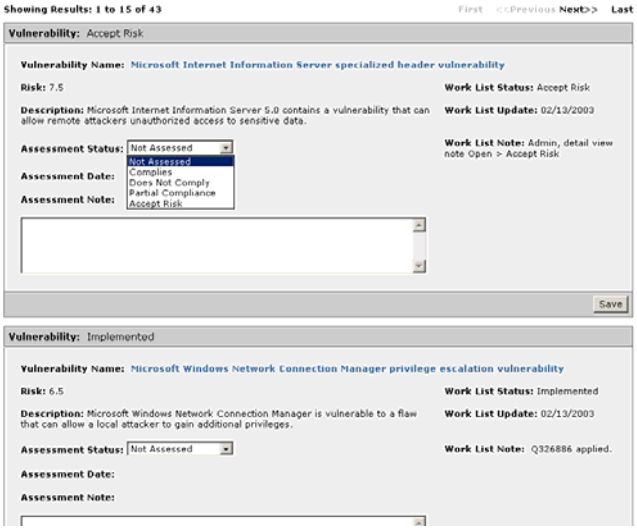
To produce an audit assessment Work Plan:

1. Perform an asset search for the appropriate asset.
2. Click the **name** of the particular asset.
3. From the Asset Detail screen, select the **Audit** tab.
4. Under the Criteria section, select the **Work List status** that is to be included in the workplan for Vulnerabilities and/or Configuration Standards.
5. Under Criteria, select the **Assessment Status** for each task that is to be included in the workplan.
6. Click **Create Workplan** and the workplan is displayed.

From the Workplan:

The Workplan displays a list of all tasks that have been closed and the user can work through each of the items on the Workplan.

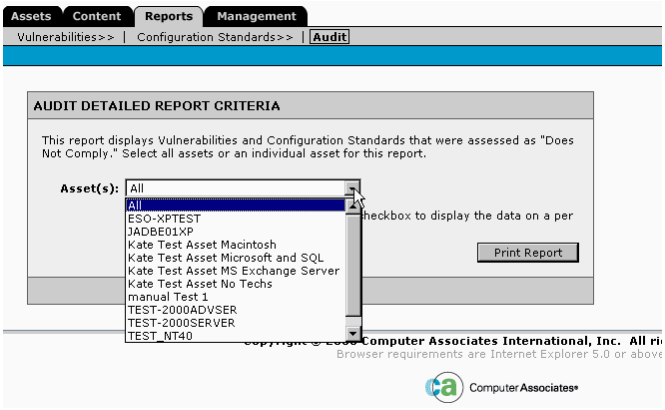
1. In the **Assessment Status field**, select a status from the drop down menu. Choices are:
   --Not Assessed
   --Complies
   --Does Not Comply
   --Partially Complies"
   --Accept Risk
2. Click **Save** to save changes to the assessment status of each task.
3. Click the **Name** link to view the Vulnerability or Configuration Standard details of a specific work plan item.



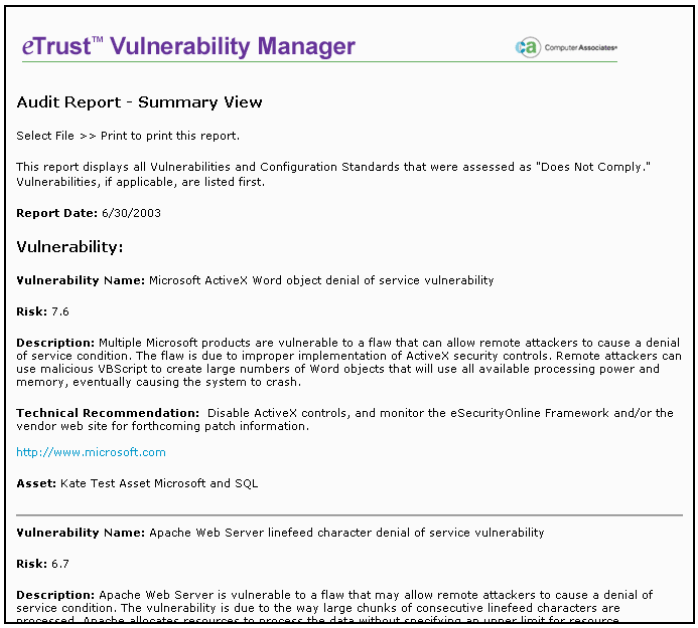
AUDITING REPORTS

The Audit Detailed report is available under the Report Tab. See the reporting section for more information on these reports.

Available audit reports include 1) a detailed listing of an audit assessment, (sorted by asset), and 2) a summary listing, sorted by Vulnerability and Configuration Standard.



An example of an Audit report is shown below.



eTrust™ Vulnerability Manager

Audit Report - Summary View

Select File >> Print to print this report.

This report displays all Vulnerabilities and Configuration Standards that were assessed as "Does Not Comply." Vulnerabilities, if applicable, are listed first.

Report Date: 6/30/2003

Vulnerability:

Vulnerability Name: Microsoft ActiveX Word object denial of service vulnerability

Risk: 7.6

Description: Multiple Microsoft products are vulnerable to a flaw that can allow remote attackers to cause a denial of service condition. The flaw is due to improper implementation of ActiveX security controls. Remote attackers can use malicious VBScript to create large numbers of Word objects that will use all available processing power and memory, eventually causing the system to crash.

Technical Recommendation: Disable ActiveX controls, and monitor the eSecurityOnline Framework and/or the vendor web site for forthcoming patch information.

http://www.microsoft.com

Asset: Kate Test Asset Microsoft and SQL

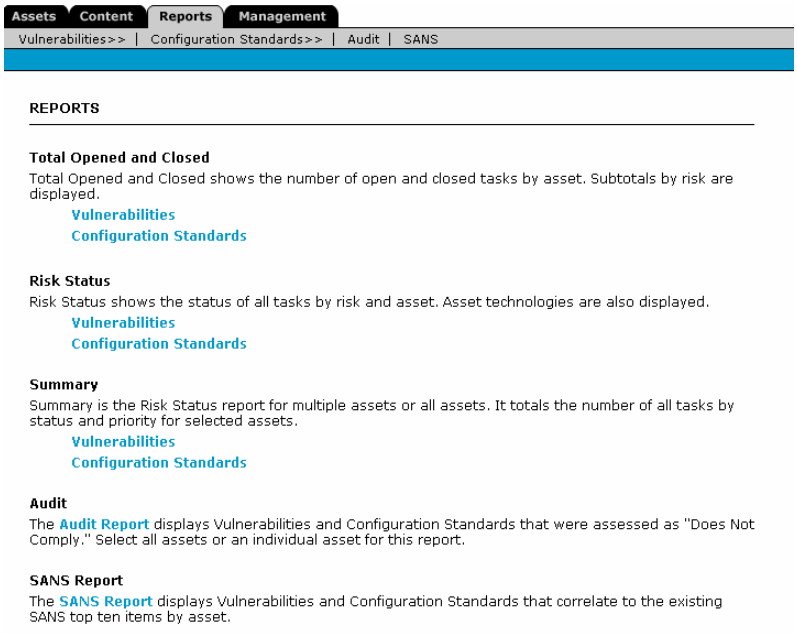
Vulnerability Name: Apache Web Server linefeed character denial of service vulnerability

Risk: 6.7

Description: Apache Web Server is vulnerable to a flaw that may allow remote attackers to cause a denial of service condition. The vulnerability is due to the way large chunks of consecutive linefeed characters are

REPORTS

eTrust VM allows users to report on eTrust VM assets. Information available includes:



The following reports are available for Vulnerabilities and Configuration Standards.

The **Total Open and Closed** report is an assessment report that shows all open and closed Vulnerability or Configuration Standard tasks for the managed assets in eTrust VM. The report is a table format grouped by status and risk of the task.

The **Risk Status** report shows the status of all Vulnerability and Configuration Standard tasks, by priority, for the managed assets in eTrust VM. Asset technologies are also displayed. This report is in a table format.

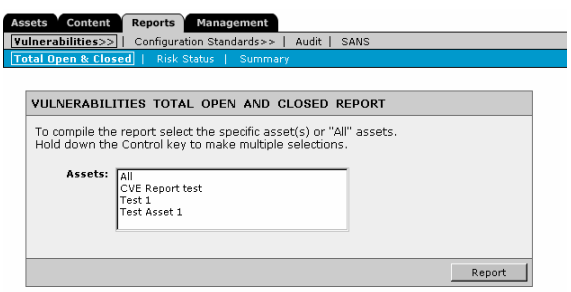
The **Summary** report summarizes the Risk Status report by displaying the status of all Vulnerability and Configuration Standard tasks, by priority, for the managed assets in eTrust VM. This summary is not asset specific.

The **Audit Report** displays Vulnerabilities and Configuration Standards that were assessed as 'Does Not Comply'. Select all assets or an individual asset from this report.

The **SANS Report** displays the assets that are affected by the top 10 Windows and Unix Vulnerabilities and Configuration Standards, as reported by the SANS Organization. The report can be grouped by asset or by SANS ID.

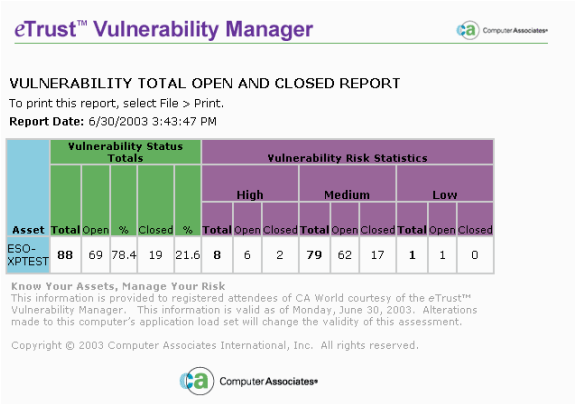
TO VIEW REPORTS:

1. Select the **Reports** tab.
2. Select the report that you would like to view.
3. Select a specific Asset or select **All** to receive a report on all managed assets.
4. Click the **Report** button to view the report.



To **print** a report, go to File menu of your browser and click Print.

EXAMPLE VULNERABILITY REPORTS:



eTrust™ Vulnerability Manager

VULNERABILITY TOTAL OPEN AND CLOSED REPORT

To print this report, select File > Print.

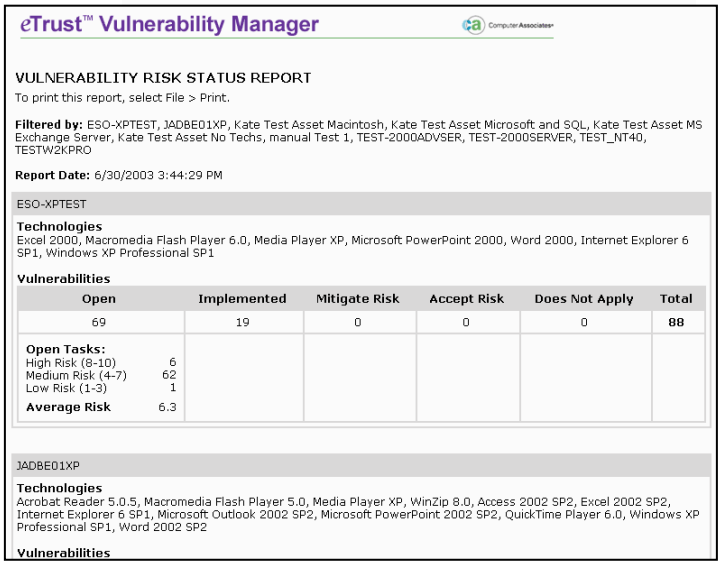
Report Date: 6/30/2003 3:43:47 PM

	Vulnerability Status Totals					Vulnerability Risk Statistics								
						High			Medium			Low		
Asset	Total	Open	%	Closed	%	Total	Open	Closed	Total	Open	Closed	Total	Open	Closed
ESO-XPTEST	88	69	78.4	19	21.6	8	6	2	79	62	17	1	1	0

Know Your Assets, Manage Your Risk

This information is provided to registered attendees of CA World courtesy of the eTrust™ Vulnerability Manager. This information is valid as of Monday, June 30, 2003. Alterations made to this computer's application load set will change the validity of this assessment.

Computer Associates



eTrust™ Vulnerability Manager

VULNERABILITY RISK STATUS REPORT

To print this report, select File > Print.

Filtered by: ESO-XPTEST, JADBE01XP, Kate Test Asset Macintosh, Kate Test Asset Microsoft and SQL, Kate Test Asset MS Exchange Server, Kate Test Asset No Techs, manual Test 1, TEST-2000ADVSER, TEST-2000SERVER, TEST_NT40, TESTW2KPRO

Report Date: 6/30/2003 3:44:29 PM

ESO-XPTEST

Technologies

Excel 2000, Macromedia Flash Player 6.0, Media Player XP, Microsoft PowerPoint 2000, Word 2000, Internet Explorer 6 SP1, Windows XP Professional SP1

Vulnerabilities

Open	Implemented	Mitigate Risk	Accept Risk	Does Not Apply	Total
69	19	0	0	0	88

Open Tasks:

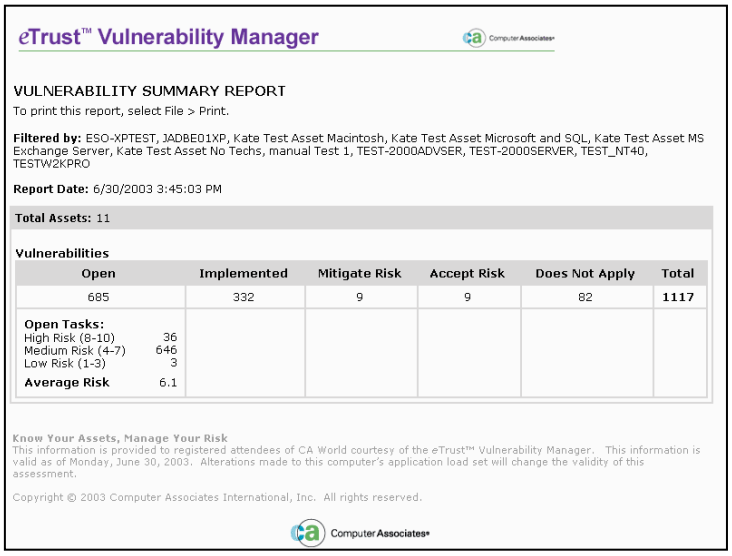
High Risk (8-10)	6
Medium Risk (4-7)	62
Low Risk (1-3)	1
Average Risk	6.3

JADBE01XP

Technologies

Acrobat Reader 5.0.5, Macromedia Flash Player 5.0, Media Player XP, WinZip 8.0, Access 2002 SP2, Excel 2002 SP2, Internet Explorer 6 SP1, Microsoft Outlook 2002 SP2, Microsoft PowerPoint 2002 SP2, QuickTime Player 6.0, Windows XP Professional SP1, Word 2002 SP2

Vulnerabilities



eTrust™ Vulnerability Manager

VULNERABILITY SUMMARY REPORT

To print this report, select File > Print.

Filtered by: ESO-XPTEST, JADBE01XP, Kate Test Asset Macintosh, Kate Test Asset Microsoft and SQL, Kate Test Asset MS Exchange Server, Kate Test Asset No Techs, manual Test 1, TEST-2000ADVSER, TEST-2000SERVER, TEST_NT40, TESTW2KPRO

Report Date: 6/30/2003 3:45:03 PM

Total Assets: 11

Vulnerabilities

Open	Implemented	Mitigate Risk	Accept Risk	Does Not Apply	Total
685	332	9	9	82	1117

Open Tasks:

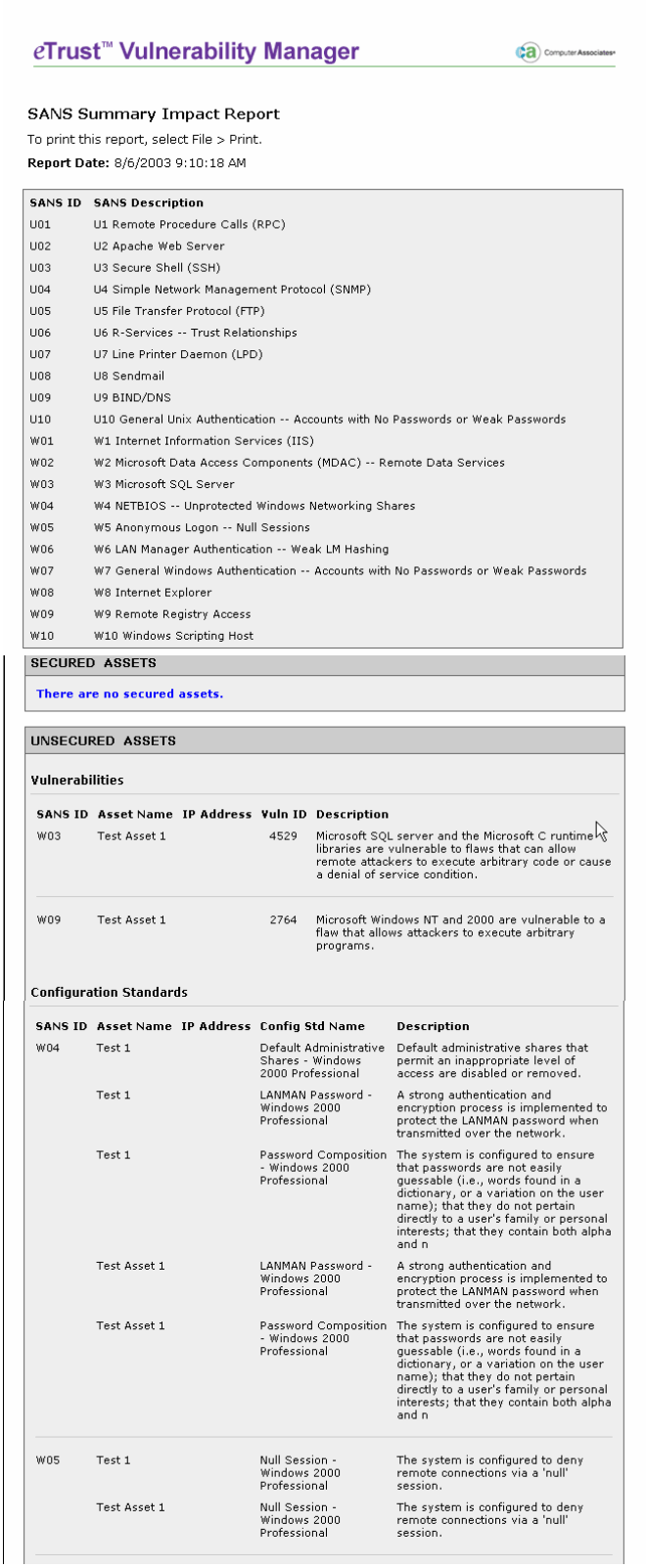
High Risk (8-10)	36
Medium Risk (4-7)	646
Low Risk (1-3)	3
Average Risk	6.1

Know Your Assets, Manage Your Risk

This information is provided to registered attendees of CA World courtesy of the eTrust™ Vulnerability Manager. This information is valid as of Monday, June 30, 2003. Alterations made to this computer's application load set will change the validity of this assessment.

Computer Associates

EXAMPLE SANS REPORT:



eTrust™ Vulnerability Manager

SANS Summary Impact Report

To print this report, select File > Print.

Report Date: 8/6/2003 9:10:18 AM

SANS ID	SANS Description
U01	U1 Remote Procedure Calls (RPC)
U02	U2 Apache Web Server
U03	U3 Secure Shell (SSH)
U04	U4 Simple Network Management Protocol (SNMP)
U05	U5 File Transfer Protocol (FTP)
U06	U6 R-Services -- Trust Relationships
U07	U7 Line Printer Daemon (LPD)
U08	U8 Sendmail
U09	U9 BIND/DNS
U10	U10 General Unix Authentication -- Accounts with No Passwords or Weak Passwords
W01	W1 Internet Information Services (IIS)
W02	W2 Microsoft Data Access Components (MDAC) -- Remote Data Services
W03	W3 Microsoft SQL Server
W04	W4 NETBIOS -- Unprotected Windows Networking Shares
W05	W5 Anonymous Logon -- Null Sessions
W06	W6 LAN Manager Authentication -- Weak LM Hashing
W07	W7 General Windows Authentication -- Accounts with No Passwords or Weak Passwords
W08	W8 Internet Explorer
W09	W9 Remote Registry Access
W10	W10 Windows Scripting Host

SECURED ASSETS

There are no secured assets.

UNSECURED ASSETS

Vulnerabilities

SANS ID	Asset Name	IP Address	Vuln ID	Description
W03	Test Asset 1		4529	Microsoft SQL server and the Microsoft C runtime libraries are vulnerable to flaws that can allow remote attackers to execute arbitrary code or cause a denial of service condition.
W09	Test Asset 1		2764	Microsoft Windows NT and 2000 are vulnerable to a flaw that allows attackers to execute arbitrary programs.

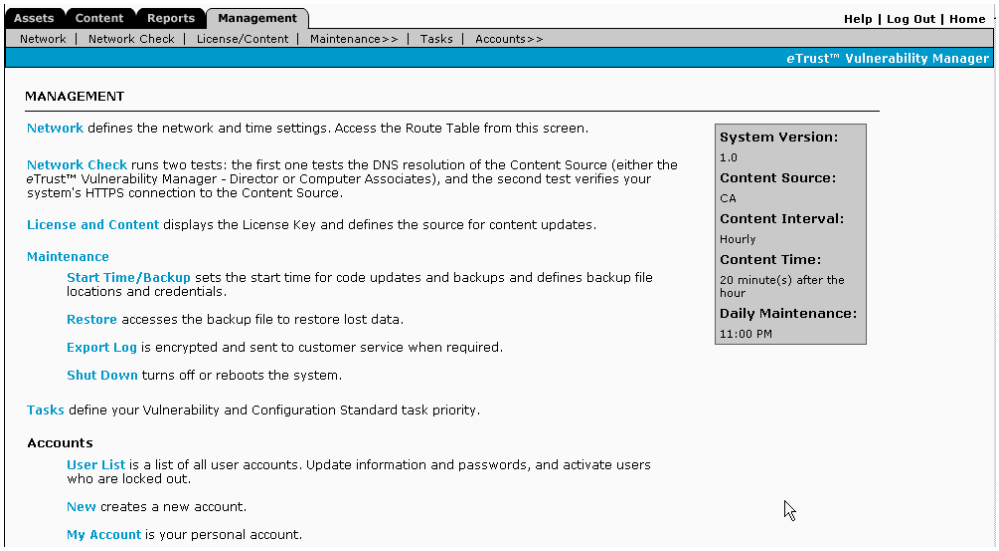
Configuration Standards

SANS ID	Asset Name	IP Address	Config Std Name	Description
W04	Test 1		Default Administrative Shares - Windows 2000 Professional	Default administrative shares that permit an inappropriate level of access are disabled or removed.
	Test 1		LANMAN Password - Windows 2000 Professional	A strong authentication and encryption process is implemented to protect the LANMAN password when transmitted over the network.
	Test 1		Password Composition - Windows 2000 Professional	The system is configured to ensure that passwords are not easily guessable (i.e., words found in a dictionary, or a variation on the user name); that they do not pertain directly to a user's family or personal interests; that they contain both alpha and n
	Test Asset 1		LANMAN Password - Windows 2000 Professional	A strong authentication and encryption process is implemented to protect the LANMAN password when transmitted over the network.
	Test Asset 1		Password Composition - Windows 2000 Professional	The system is configured to ensure that passwords are not easily guessable (i.e., words found in a dictionary, or a variation on the user name); that they do not pertain directly to a user's family or personal interests; that they contain both alpha and n
W05	Test 1		Null Session - Windows 2000 Professional	The system is configured to deny remote connections via a 'null' session.
	Test Asset 1		Null Session - Windows 2000 Professional	The system is configured to deny remote connections via a 'null' session.

MANAGEMENT TAB

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

- **Network** (defines network IP address, route tables and time settings of the appliance)
- **Network Check** -Admin 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 source for content updates {CA or eTrust VM-D})
- **Maintenance** (includes settings for start time, restore of data, troubleshooting and shutdown)
- **Tasks** (defines the settings for Vulnerability and Configuration tasks that will be generated)
- **Accounts** (displays user lists and create new accounts {admin only}, modify personal accounts).
- **Integration** (displays iRecorder functionality for integration with eTrust Audit. This is seen by the Administrator role only. See the Integration section for complete details.)



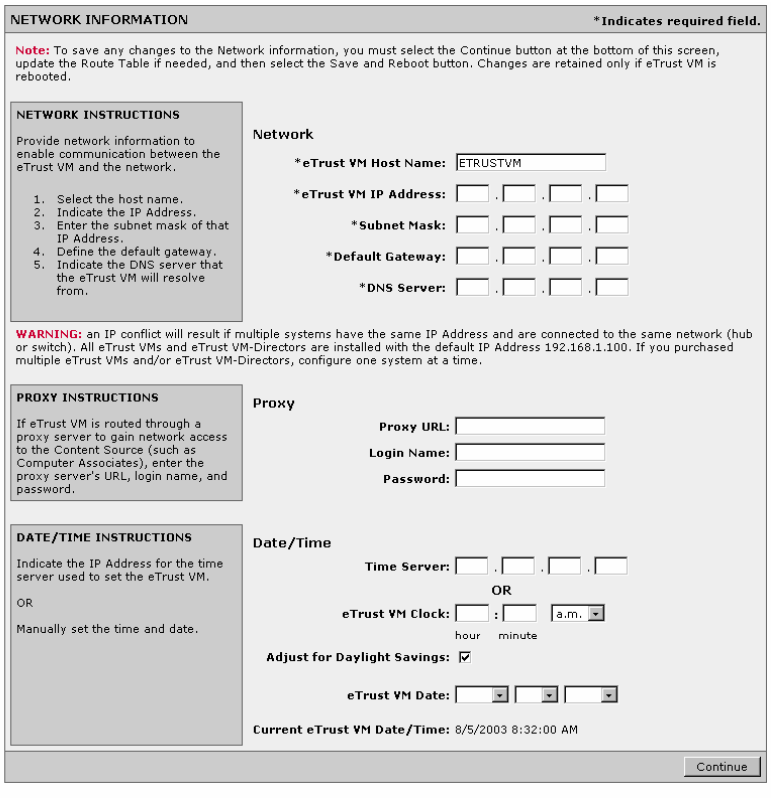
MAINTENANCE STATUS

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

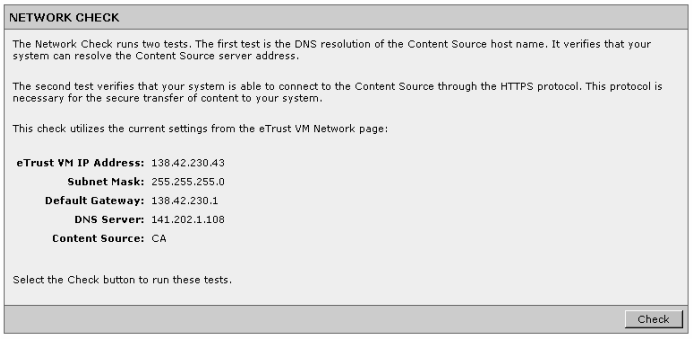
- **eTrust VM Version**. This is the version of the current eTrust VM release.
- **Content Source.** This is determined from the License/Content page settings. It will indicate either CA or the IP address of a eTrust VM-Director.
- **Content Interval.** This is determined from the License/Content page settings and will be either Daily or Hourly.
- **Content Time.** This is the actual time that the eTrust VM makes the request for content from the source (CA or eTrust VM-Director).
- **Daily Maintenance.** This is the scheduled time determined from the Start Time/Backup page settings.

NETWORK

Network information for eTrust VM was obtained during the initial setup. This information can be modified from the Management tab, but is not recommended. If IP Addresses are changed, all eTrust VM Inventory Service applications must be redeployed. See the Network Information section in the setup process for more information.



NETWORK CHECK



The Network Check function is available to the administrator role only. This check runs two tests.
The first is the DNS resolution of the Content Source (CA or eTrust VM-Director) host name. It verifies that your system can resolve the Content Source server address.

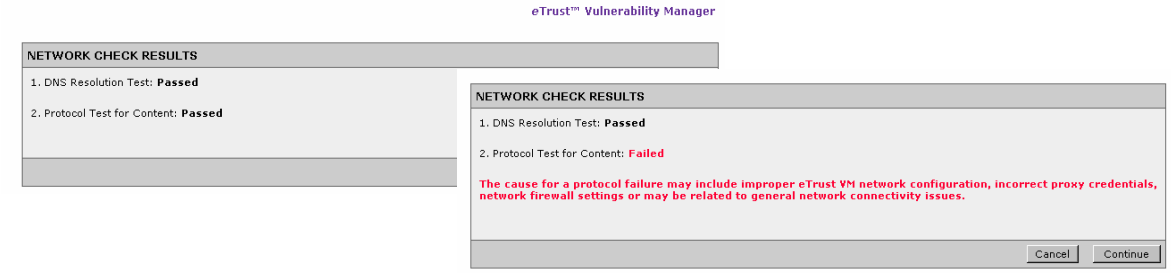
The second test verifies that your system is able to connect to the Content Source through the HTTPS Protocol. This protocol is necessary for the secure transfer of content to your system.
This check utilizes the current settings from the eTrust VM Network page (the IP values will be listed as well as the Content Source).

The **Check** button at the bottom of the page executes the network checks.

A failed protocol network check would display the following message:
The cause for a protocol failure may include improper network configuration, network firewall settings, or may be related to general network connectivity issues.

A failed DNS resolution would display the following message:
The configured DNS for the eTrust VM is unable to resolve the appropriate CA address. The cause for DNS failure may be related to eTrust VM DNS configuration or to your configured DNS server.

Troubleshooting Tip: Check your firewall settings to allow the communication. Ensure you have valid IPs set up.



LICENSE CONTENT

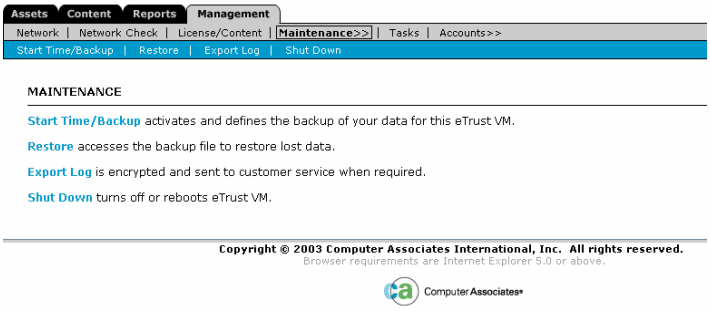
The License Key field, displayed from the Management tab, allows the user to view the License Key for this eTrust VM. This information was obtained in the setup process and cannot be modified. See the License Key section in the configuration process for more information.

MAINTENANCE

Maintenance of eTrust VM applies to code updates to the application and backup of data.

CA never "pushes" code or content to eTrust VM. eTrust VM initiates all communication and issues the requests for information. Communication between eTrust VM 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 unit to receive updates.

Content updates were scheduled during the Setup Wizard. 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. The new content and any code updates are held until the scheduled maintenance start time. The Maintenance Settings are then used to determine what time the code updates, sitting in the holding area, will actually be applied to eTrust VM. It is important to remember when scheduling that eTrust VM will be down during the time the code is applied.



Security patches are contained in maintenance code releases. All security patches are tested during the CA QA process as part of the maintenance release testing.

Only eTrust VM Administrator will have access to the Maintenance function(s). The Maintenance function will address the backup and restore procedures and define the start time to perform code updates on eTrust VM.

BACKUP SETTINGS

During the setup process, the user can elect to activate the automated daily 'Backup' of files. If backup settings ARE enabled, eTrust VM database files will be backed up as part of the maintenance process, according to the scheduled time and location (FTP or UNC). Each backup will be a separate file with a new name. If this option is NOT enabled, backup will not occur.

From the Management tab, this setting can be modified, at anytime.

1. Check the 'Inactive' radio button if backups are not to be activated
   Or, Indicate an 'Active UNC' field (ex. \\192.168.1.100\backup_share) or an 'Active FTP' field (ex. 192.168.1.100)

Indicate a secure **server location** to backup eTrust VM files to. The server location must be within the local network of eTrust VM or accessible from the route table.

Backup Credentials:

1. Enter the username and password that allows access to the backup location.

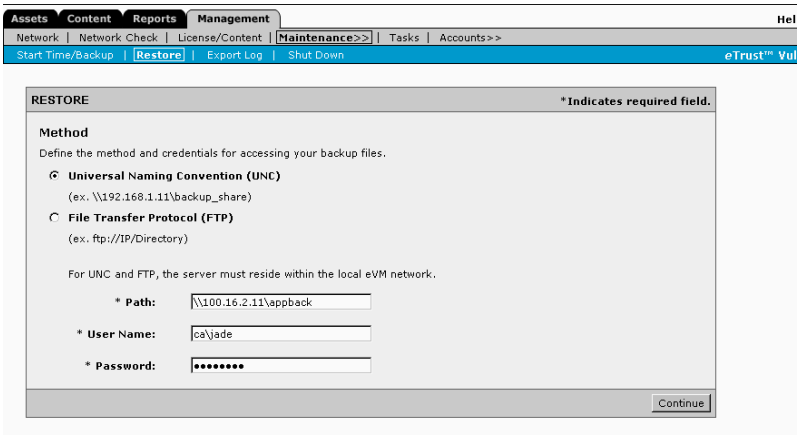
Frequency will be specified by selecting one of the following:

1. Now--This option is available only from the Management tab and not from the Setup Wizard.
2. Daily--The start time that is defined for the Maintenance window will be used as the time the backup will occur.

The backup **file name** will be auto-generated and be made up of eTrust VM name, code version and a date/time stamp.

RESTORE DATA

System restores can be performed on demand. When performing a system restore, users may select from available backup files. Partial system restores are not permitted. See the Backup Settings for complete instructions.



To Restore Data:

1. Select the Method (UNC or FTP).
2. Provide the FTP address, if selected.
3. Type the Username and Password that allows access to the selected location.
4. Click Continue.
5. After clicking the Continue button, the credentials are checked.
6. If the system cannot connect, an appropriate error message is displayed.
7. If the system is able to connect, a list of all files found on the backup location is displayed.
8. Select a file or all files and click the Restore button.
9. The user is directed to the "eTrust VM Temporarily Offline" page while the restore is being performed.

The Restore function will display a list of all files found on the device identified in the backup information (explained in the previous section). If there is a failure during the restore process, the system will *automatically* roll back to the state prior to execution of the recovery process.

Notes:

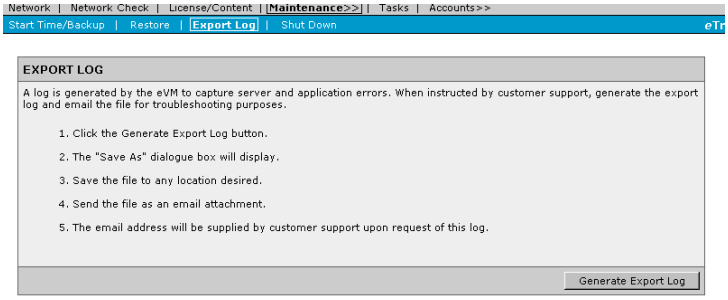
- Partial system restores are not permitted.
- If there is a failure during the restore process, the system will automatically roll back to the state prior to the restore process.
- The user has the ability to change the restore file name, but it is not recommended.
- If the restore process is interrupted,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

EXPORT LOGS

eTrust VM Administrator may export system logs in a compressed, encrypted format and send them to their Customer Support provider for troubleshooting.

A log is generated by eTrust VM 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.

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.
5. The email address will be supplied by customer support upon request of this log.



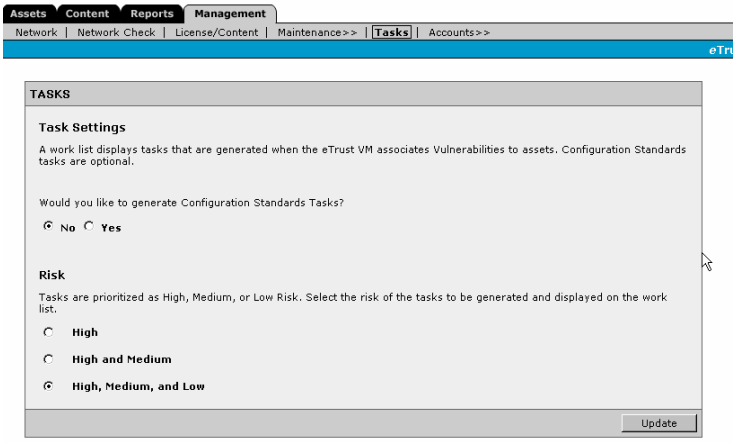
TASK SETTINGS

Task settings are determined in the initial setup of the eTrust VM but may also be modified from the Management tab. By default, the Work List will display tasks that are generated from Vulnerabilities associated to your managed assets. Configuration Standards tasks are optional and can be selected from this screen.

Tasks are prioritized by **risk level**. By default, tasks will be generated for Vulnerabilities and Configuration Standards (if applicable) with risk levels of **High, Medium and Low**. These settings are determined in the initial setup of the eTrust VM but may also be modified from the Management tab.

To change the risk level of the tasks to be included in the work list:

1. Select the appropriate **level**
2. Click **Update.**



If risk levels **change from High or High & Medium to include lower risk items**, new tasks will be generated for the appropriate assets.

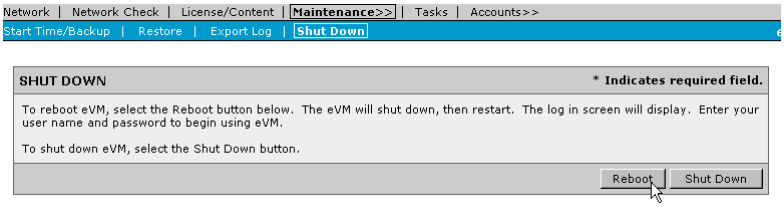
If the risk levels are **changed to exclude lower risk items**, the excluded risk items will be removed from the Work list. Any Work History (relevant & archived) associated with lower risk items would remain.

If these lower risk levels are included at a later time, eTrust VM will re-open all relevant tasks.

eTrust VM will compare against the relevant Work History and those that still apply will remain in relevant Work History. Those that no longer apply, due to a change in the asset, will be archived.

SHUT DOWN

The Shut Down screen allows eTrust VM to be shut down or rebooted.



USER ACCOUNTS

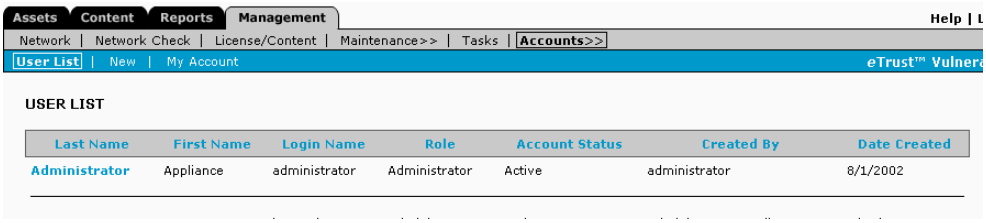
Account Administration

Administrators have access to all User Account functions.

User Account Guidelines

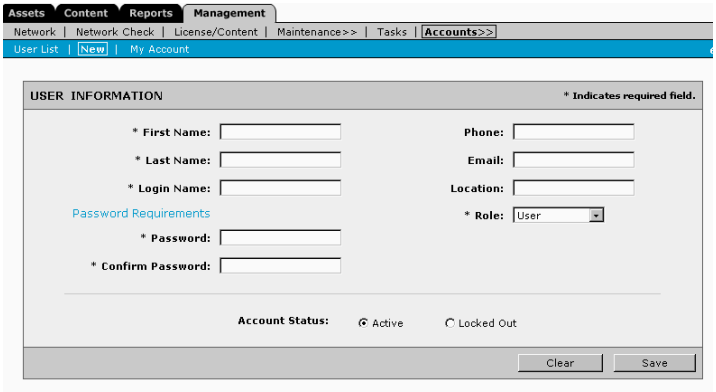
- Login names must be unique
- Login names are NOT case sensitive
- Only one Role can be assigned to each user account.
- A maximum of two eTrust VM Administrator accounts may be created.
- A maximum of fifty eTrust VM User accounts may be created, but all may not be logged on concurrently.
- New users are required to change their password upon login and will be automatically prompted.
- An eTrust VM Admin account may be deleted if there is at least one other active Administrator account.
- When a user's account is deleted, the application will unlock all tasks associated with that user.

To view all accounts for eTrust VM, select the **Accounts** link from the Management tab.



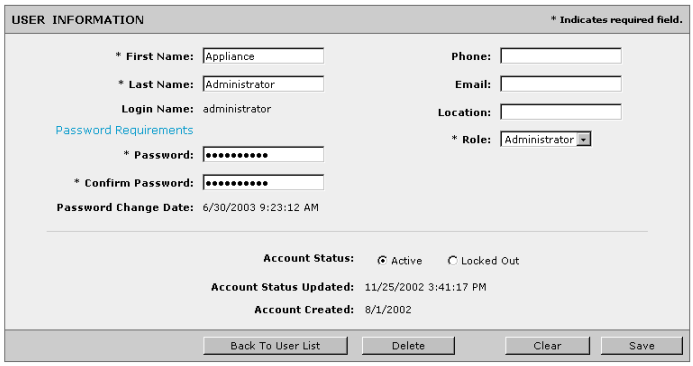
To Add a User Account:

1. Click the **New** link from the Accounts menu.
2. The New Account form is displayed.



To edit an Account:

1. Select the **Last Name** link from the list of accounts.
2. The edit form is displayed.
3. Make necessary changes and click **Save**.
   Or, click **Delete** to remove this user (any tasks locked by the user will be unlocked).



5. Complete the following fields to create a new eTrust VM user.
   - First Name, Last Name and Login Name- required fields
   - Password – click the 'Password Requirements' link as a guide, required field
   - Confirm Password – re-type the password, required field
   - Phone – optional field
   - E-mail address – optional field
   - Location – optional field
   - Role – select the role from the dropdown menu, user or administrator (fifty users and two administrators are allowed)
   - Account Status – by default, the Active radio button will be selected
6. Click **Save** to create the account.

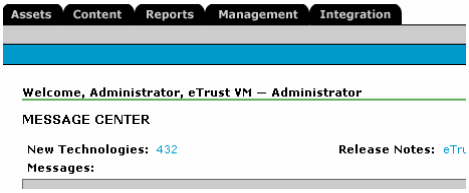
Upon login, the user will be prompted to change their password.

To View or Edit your User Account:

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

iRECORDER INTEGRATION

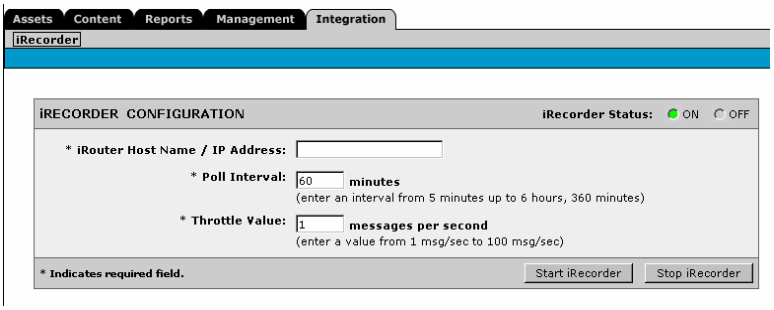
eTrust VM integrates with eTrust Audit by capturing events and mapping them thru iRecorder to eTrust Audit. Audit then integrates to eTrust Security Command Center. This functionality is available and viewable to the **Administrator Role only**.



WARNING: DO NOT attempt to use this function if all integrations points have not been setup with eTrust Audit.

To begin processing event data to iRecorder:

1. Input the **iRouter Host Name OR the IP Address,** only one may be specified.
2. Define the **Poll Interval** in Minutes-This determines how often to package and send the event data (5 minutes minimum to 360 minutes maximum).
3. Define the **Throttle Value**- This determines how many messages to send (1 msg per second minimum to 100 messages per second maximum).
4. Click **Start iRecorder**.
5. The **iRecorder Status** green indicator will switch to **On**.
6. The values will be sent to the configuration file and event data will be processed on schedule without further intervention.



EVENT DATA CAPTURED

There are nine types of events captured by eTrust VM and sent to eTrust Audit, via iRecorder.

1. **Auto Discovery** – events sent when a new asset is discovered via Auto Discovery
2. **Asset Added** – events sent when an asset is created by any method (manually or via Auto Inventory)
3. **Asset Modified** – events sent when an asset is modified
4. **Asset Deleted** – events sent when an asset is deleted
5. **Asset Managed** – events sent when the communication is enabled between the Service on the asset and the eTrust VM
6. **Asset Unmanaged** – events sent when the communication is disabled between the Service on the asset and the eTrust VM
7. **Asset New Technology** – events sent when a new technology is added, manually or through the Service
8. **Asset Remove Technology** – events sent when a technology is removed, manually or through the Service
9. **Asset New Vulnerability** – events are sent when a new vulnerability is detected for an asset

FREQUENTLY ASKED QUESTIONS/TROUBLESHOOTING

For additional help with configuration, setup, functionality and other issues of the eTrust™ Vulnerability Manager, see the Troubleshooting section of the Help Files in the eTrust VM application. FAQs are also posted on the Computer Associates website at http://esupport.ca.com. You may also contact a Computer Associates Support representative for additional assistance by calling 1-631-342-5803.