Faronics

DEEP FREEZE™

ABSOLUTE Workstation Integrity

Deep Freeze Enterprise - Computer Associates eTrust Antivirus

TECHNICAL WHITEPAPER

Last modified: September 28, 2007

Faronics

Toll Free Tel: 800-943-6422
Toll Free Fax: 800-943-6488
International Tel: +1 604-637-3333
International Fax: +1 604-637-8188

www.faronics.com

Faronics™

Introduction

The process of updating virus definitions on workstations protected by Deep Freeze Enterprise involves three fundamental steps:

1. Rebooting the workstations into a *Thawed* state so the updates are kept upon restart
2. Updating the virus definitions
3. Shutting down or restarting the workstation into a *Frozen* state

This white paper provides technical information on how to approach these steps with CA's eTrust Antivirus.

Deep Freeze is not marketed as an antivirus product. However, Deep Freeze will protect workstations from any virus. Just restart the Frozen workstation and the virus is gone. Many viruses require a fundamental change to be made to the core files and only become active on restart. With Deep Freeze installed and activated, these viruses will be deleted upon restart and therefore never become active.

Ensure the BIOS is set to boot directly to the C: drive and that the BIOS is protected with a password; failure to do so can result in boot sector viruses being transferred to the hard disk drives via infected floppy disks.

Setting the Workstations to a Thawed state

In order to make any permanent changes, the workstations protected by Deep Freeze have to be set into a *Thawed* state. Those permanent changes include antivirus updates; therefore, the workstations must be rebooted into a *Thawed* state before applying these updates.

There are three ways to remotely set workstations into a *Thawed* state:

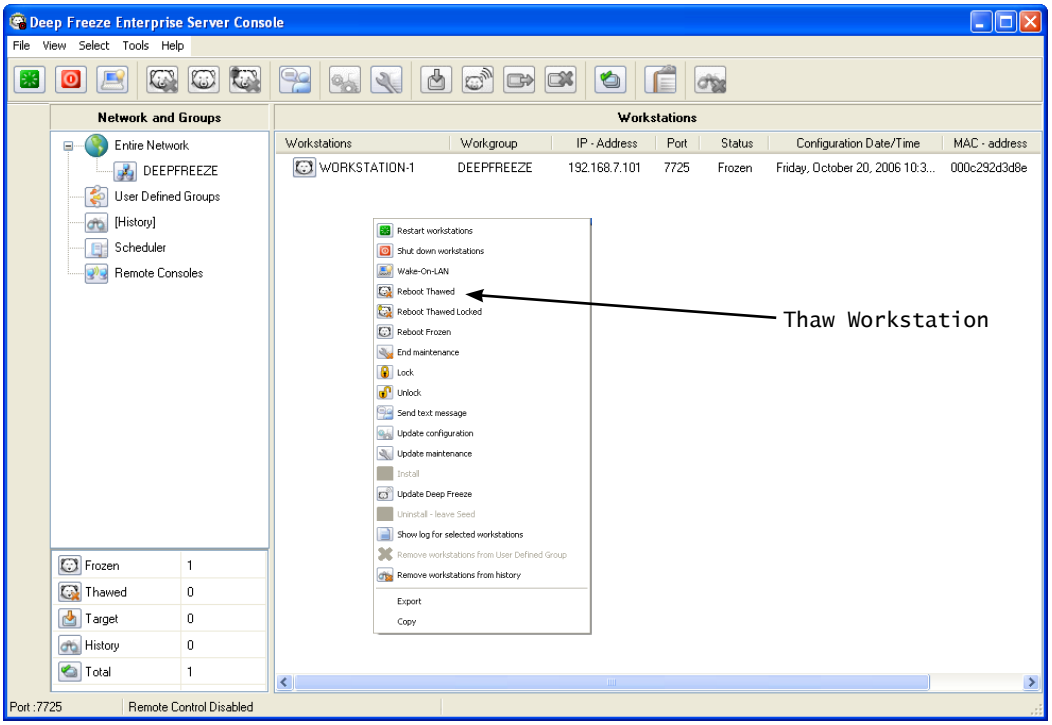
- By manually using the Deep Freeze Enterprise Console
- By setting up an Scheduled Maintenance Period
- By using the Command Line Control

Manually Using the Deep Freeze Enterprise Console

The Enterprise Console contains a toolbar at the top of the screen that allows quick access to the functions of the Console.

To boot a workstation into the *Thawed* state, select the workstation and click the *Thaw Workstation* icon on the toolbar.

Alternatively, right-click and select the *Set Computer(s) to Thaw* option in the context menu.



Click *OK* in the confirmation window.

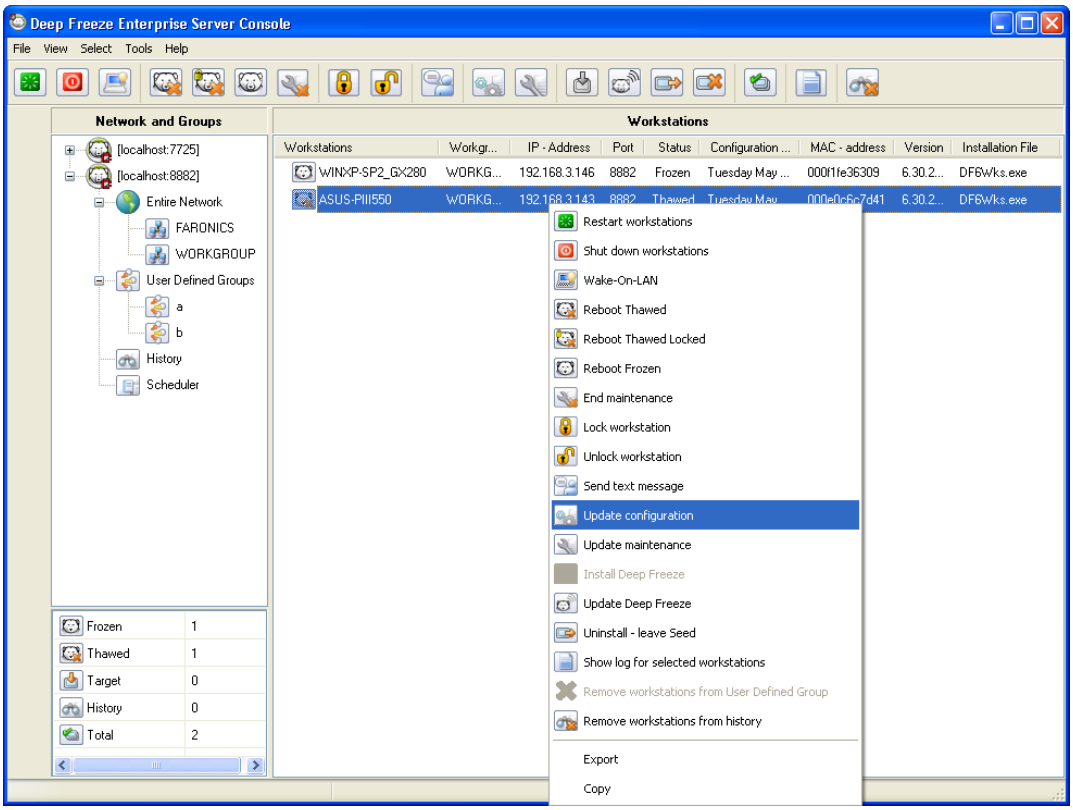
The selected workstations now restart in the *Thawed* state.

Setting up a Scheduled Maintenance Period

There are two ways to set up a Scheduled Maintenance Period. One is to set it up when configuring the Deep Freeze Enterprise installation files with the Configuration Administrator (best method for new deployments) and the other way is to create or update the Maintenance Period using the Enterprise Console.

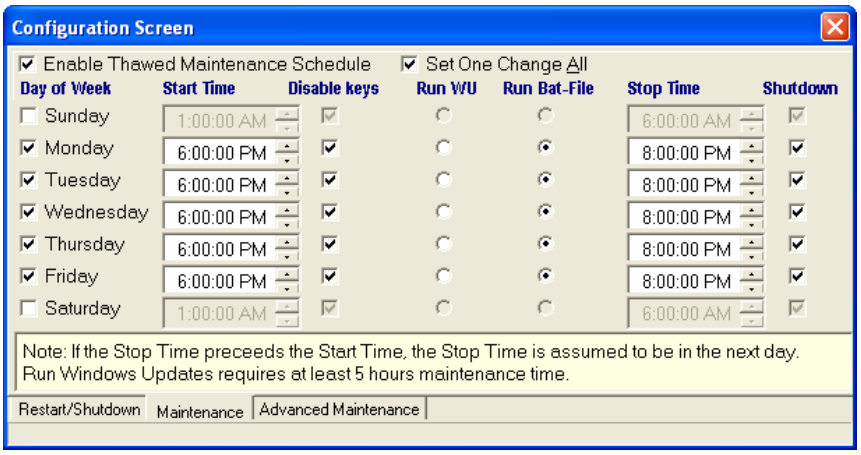
Assuming you have already deployed Deep Freeze throughout your network, the following instructions elaborate on how to create/update the Maintenance Period with the Enterprise Console.

1. Open the Enterprise Console. Select any workstation and right-click on it.
2. Select *Update Maintenance Period.*



A toolbar appears at the bottom of the screen.

3. Click *New*. The *Configuration Screen* appears as shown. It only contains the *Restart/Shutdown*, *Maintenance* and *Advanced Maintenance* options.



4. Click on the *Maintenance* tab and place a check in the *Enable Thawed Maintenance Schedule* check box. Also place a check beside each day you want the Maintenance Schedule to run.
5. Set the Maintenance start time for each day in the *Start Time* column, and the end time in the *Stop Time* column.
6. It is recommended that the *Disable keys* option is checked so the keyboard and mouse are disabled while the workstations are in the *Thawed* state.

   It is also important to check the *Shutdown* box so Deep Freeze shuts the workstations down at the end of the Maintenance Period. Otherwise the workstations are restarted after the Maintenance Period is complete.
7. Close the *Configuration Screen*. A pop-up message appears, requesting the administrator to select the workstations to send the new configuration to.
8. Select the workstations to be updated and click *Send*. This action updates all the selected workstations' configuration on the fly. This means the workstations don't have to be in the *Thawed* state for the configuration updates to take place.

Controlling Deep Freeze Through the Command Line Control - DFC

The Deep Freeze *Command Line Control* (*DFC*) offers network administrators increased flexibility in managing Deep Freeze workstations. DFC works in combination with third-party enterprise management tools and/or central management solutions. This combination allows administrators to update workstations on the fly and on demand.

It is important to note that DFC is not a stand-alone application. DFC integrates seamlessly with any solution that can run script files, including standard run-once login scripts.

DFC commands require a password with command line rights. OTPs cannot be used.

List all commands by calling DFC without parameters.

The files are copied to *C:\WINDOWS\system32\DFC.exe*

DFC Boot Control

Syntax	Description
DFC password /BOOTTHAWED	Restarts workstation into a Thawed state. Only works on Frozen workstations.
DFC password /THAWNEXTBOOT	Sets up workstation to restart Thawed the next time it restarts. Only works on Frozen workstations. Does not force workstation to restart.
DFC password /BOOTFROZEN	Restarts workstation into a Frozen state. Only works on Thawed workstations.
DFC password /FREEZENEXTBOOT	Sets up workstation to restart Frozen the next time it restarts. Only works on Thawed workstations. Does not force workstation to restart.

DFC Status Query

Syntax	Description
DFC get /ISFROZEN	Queries workstation if it is Frozen. Returns 0 if Thawed. Returns 1 if Frozen.

Configuration Update

Syntax	Description
DFC password /CFG=[path] depfrz.rdx	Replaces Deep Freeze configuration information. Works on Thawed or Frozen workstations. Password changes are effective immediately. Other changes require restart.

Example Batch File

Below is a sample batch file that can be modified for use with any antivirus software that supports updating through a command line.

```
@ECHO OFF
\\SERVER\SHARE\FOLDER\DFC.EXE get /isfrozen
IF ERRORLEVEL 1 GOTO FROZEN
IF ERRORLEVEL 0 GOTO THAWED
ECHO Errors where encountered running the command line control on this workstation.
:FROZEN
\\SERVER\SHARE\FOLDER\DFC.EXE password /bootthawed
GOTO END
:THAWED
REM ************************************************************************
REM * Insert the command to update the antivirus software here.  *
REM ************************************************************************
\\SERVER\SHARE\FOLDER\DFC.EXE password /freezenextboot
REM Send commands to reboot the system.
REM For Windows 95/98/ME
RUNDLL32 SHELL32.DLL,SHExitWindowsEx 2
REM For Windows 2000 (may need to be called 2x)
RUNDLL32 USER32.DLL,ExitWindowsEx 2
RUNDLL32 USER32.DLL,ExitWindowsEx 2
REM For Windows XP
SHUTDOWN -s -t 01
GOTO END
:END
```

Updating the Virus Definitions

This document provides three different ways to approach virus signature file updates for CA eTrust Antivirus clients.

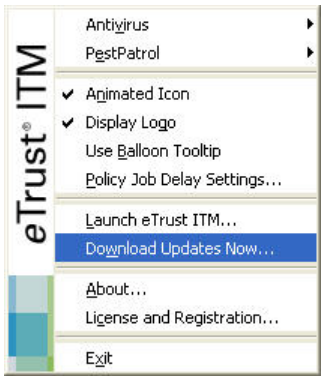
1) Do Nothing

The virus signature file continues getting updated every time the workstations are restarted or whenever the updates are pushed down, but the changes are lost upon reboots. On fast-switched networks this has a negligible impact on the boot-up time.

The workstations have the latest definitions at all times. The only downside of this method is that, with time, the signature file keep growing bigger. Therefore, it is recommended to schedule a *Thawed* Maintenance Period at least twice a year to make the updates permanent.

2) Manually Update the New Virus Definitions

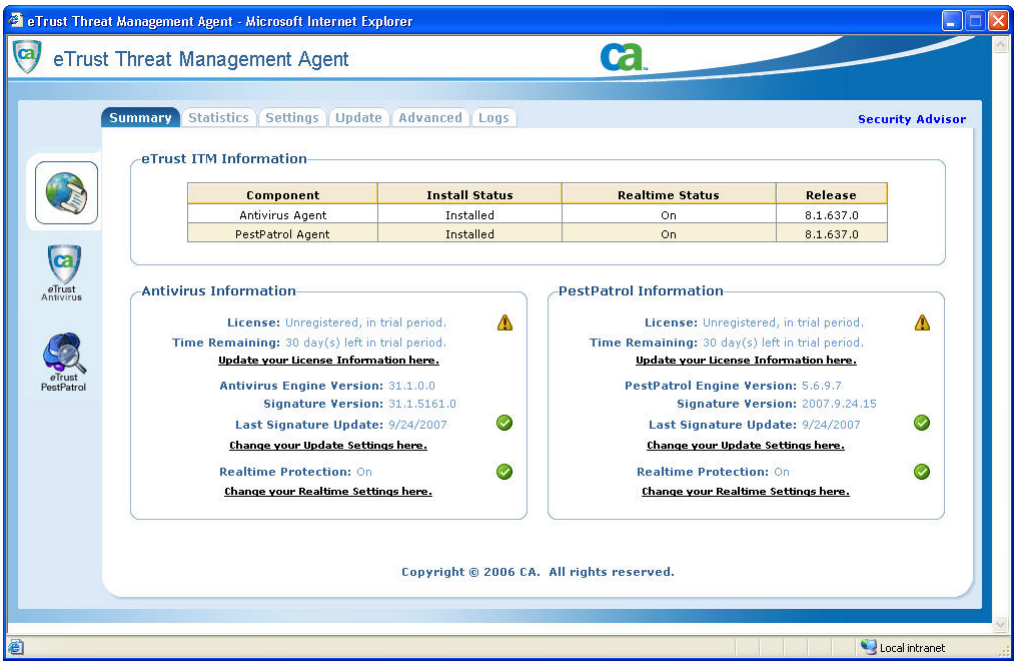
1. Using the Deep Freeze Enterprise Console, set the workstations to reboot into the Thawed state.
2. When the computers are back on, right click the eTrust icon on the system tray to access the menu.
3. Select *Download Updates Now,* this will automatically download and apply updates from the distribution server as shown below.



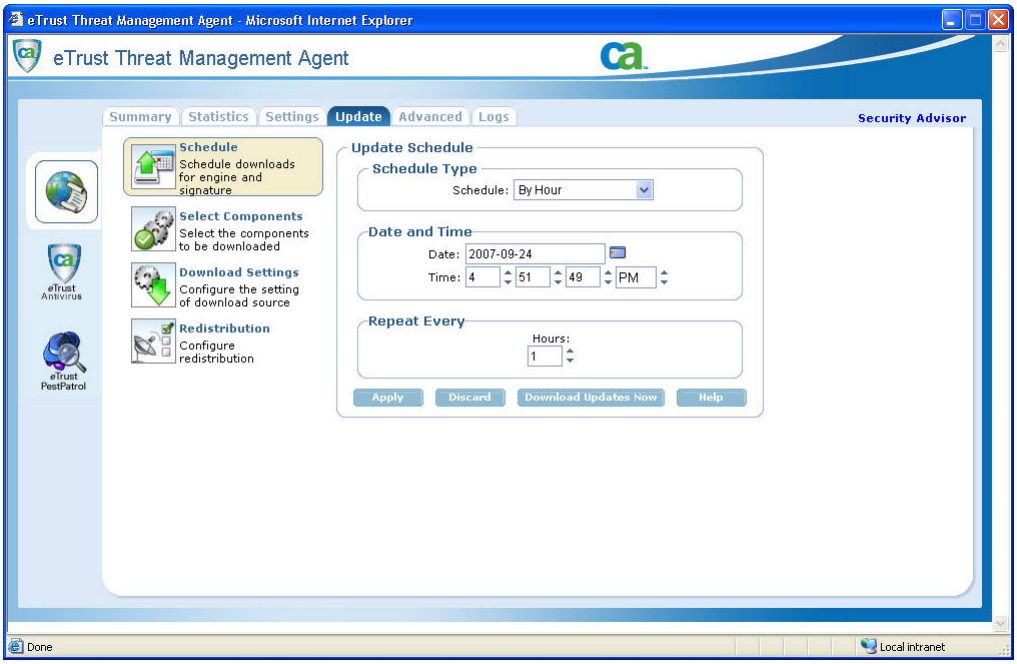
This immediately updates the Virus Signatures.

3) Scheduling the Virus Updates From the Local Computer

1. Using the Deep Freeze Enterprise Console, schedule a Maintenance Period as per instructions provided on p. 4-5.
2. Right click the eTrust icon on the system tray and choose *About* on the menu.
3. On the *Summary* page, click on *Change your update settings here.*

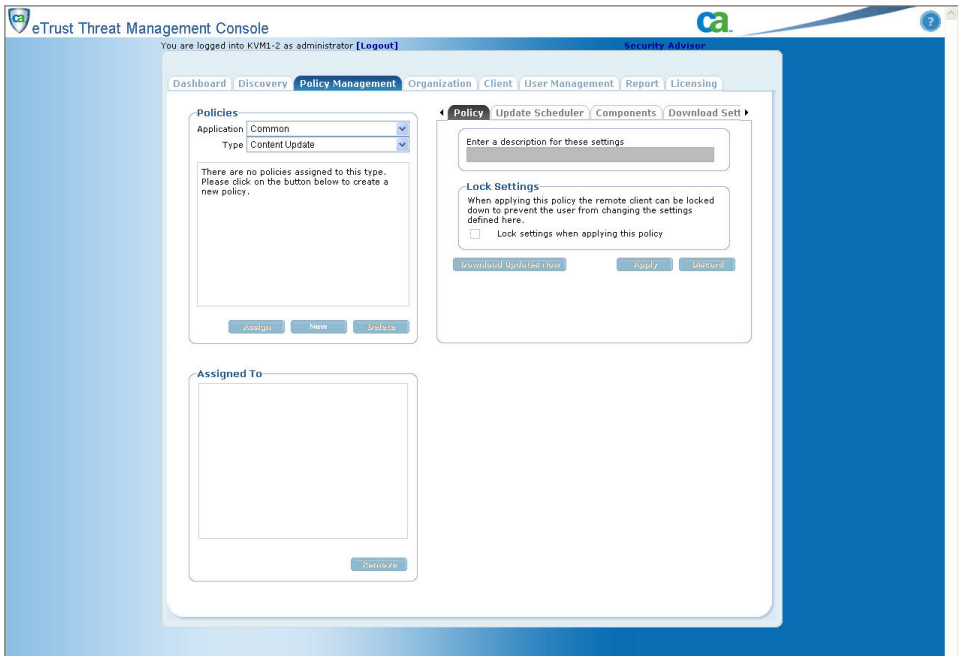


4. On the *Update* tab set the date and time that updates will be downloaded to correspond with the date and time of the Maintenance period configured in step 1.

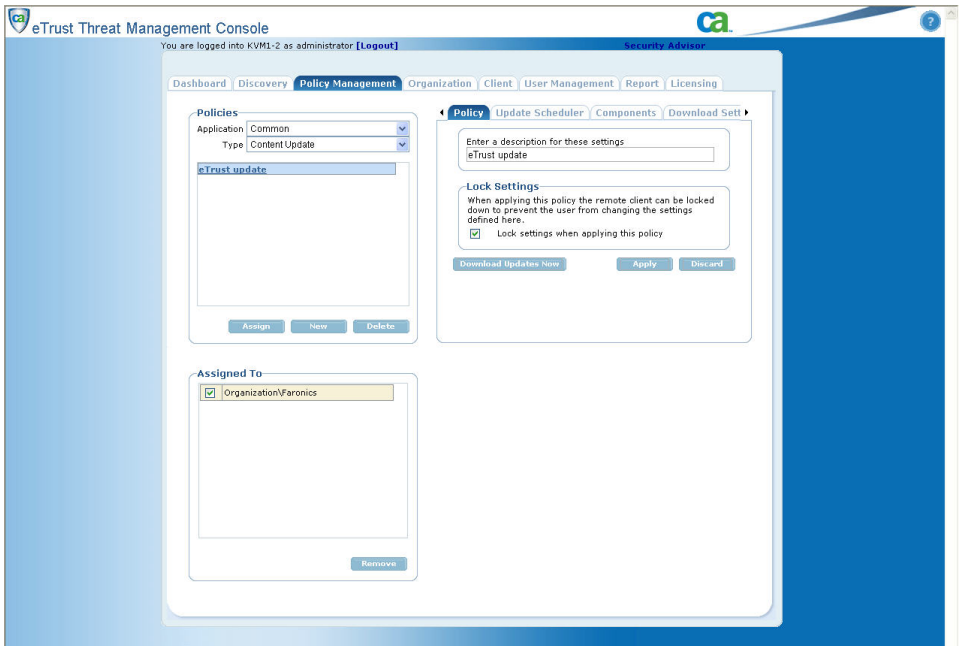


4) Scheduling the Virus Updates from eTrust Threat Management Console

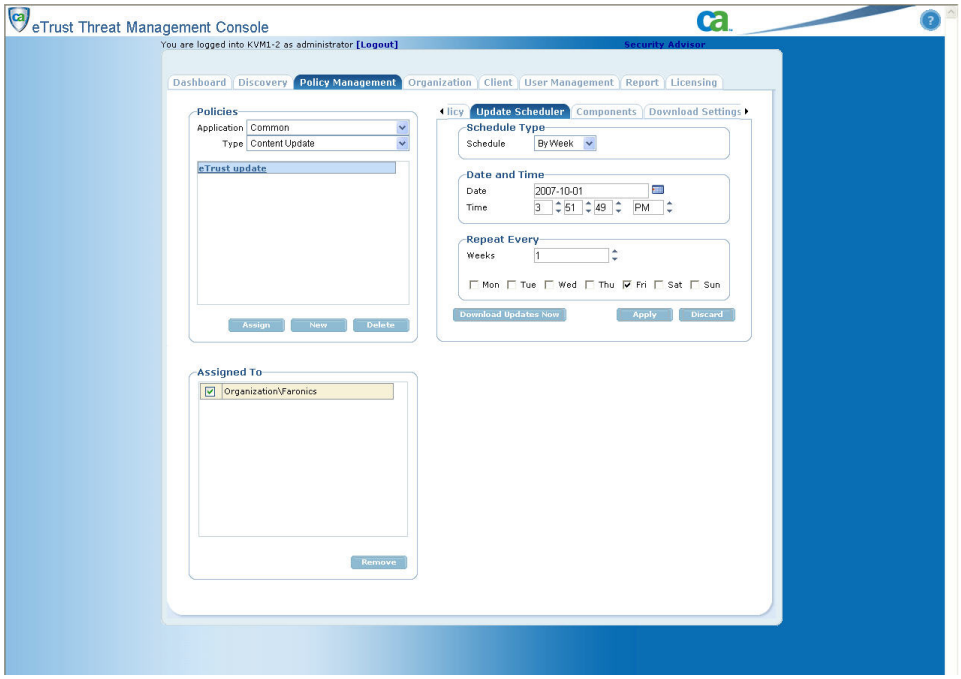
1. Using the Deep Freeze Enterprise Console, schedule a Maintenance Period as per instructions provided on p. 4-5.
2. Open the eTrust Threat Management Console and click on the *Policy Management* tab



3. On the *Policy Management* tab select *Common* on the *Applications* drop down menu, and then select *Content Update* on the *Type* menu and click on *New* to create a new policy. Enter a description of the policy and assign the policy to the organization containing the computers to be updated.



4. Click on the *Update Scheduler* tab and set the schedule to match the settings for the Maintenance period specified in step one.



5. Click on the *Components* tab and select the eTrust components that you want to update. When the appropriate settings have been selected click *Apply* to finish.