ENTERPRISE SECURITY

PRODUCT MANUAL

v.2012.1.11

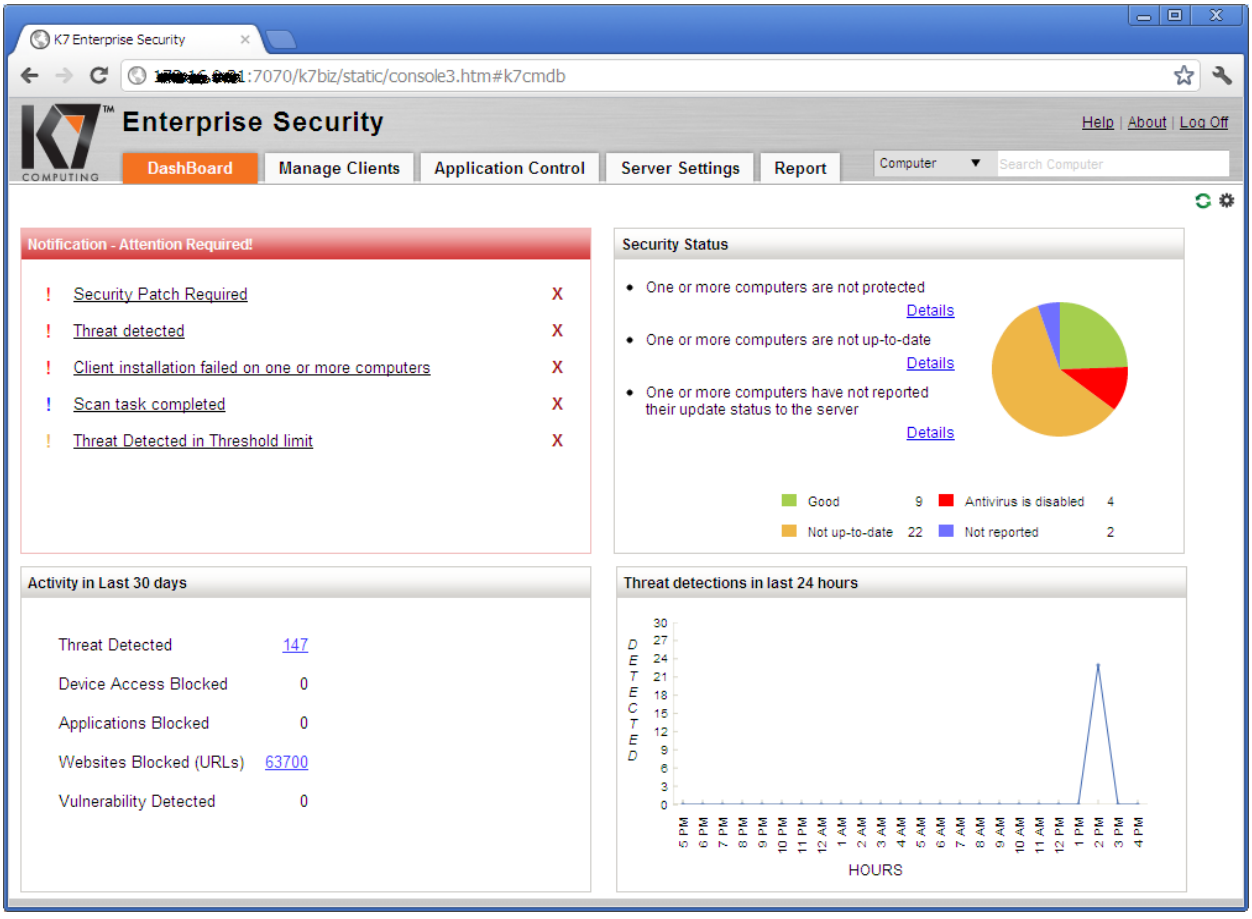
TABLE OF CONTENTS

ABOUT THE ADMIN CONSOLE

The Admin Console is a centralized web-based management console. The web console is accessible through most web browsers (MS Explorer, Google Chrome, Mozilla Firefox, Apple Safari, etc.) from any computer within the network. Administrators can manage the entire security settings - including client installations, managing Groups, Policies, Tasks, updates, Antivirus, Firewall, Application Control, Web Filtering, Notifications,etc.

DASHBOARD

Dashboard is the main console where the administrator can have a quick glimpse at K7 Endpoint client's security status including Threat Detection, Update Status, Scan Task Completion status, Client installation/un-installation status, Antivirus/Firewall protection status, Device Access violations, Applications/Websites blocked, Vulnerability Detection, Subscriptions, etc. Administrators can quickly navigate from the dashboard to potential problematic areas by clicking on the corresponding issue link, this will bring up a detailed report and an up-to-date status.



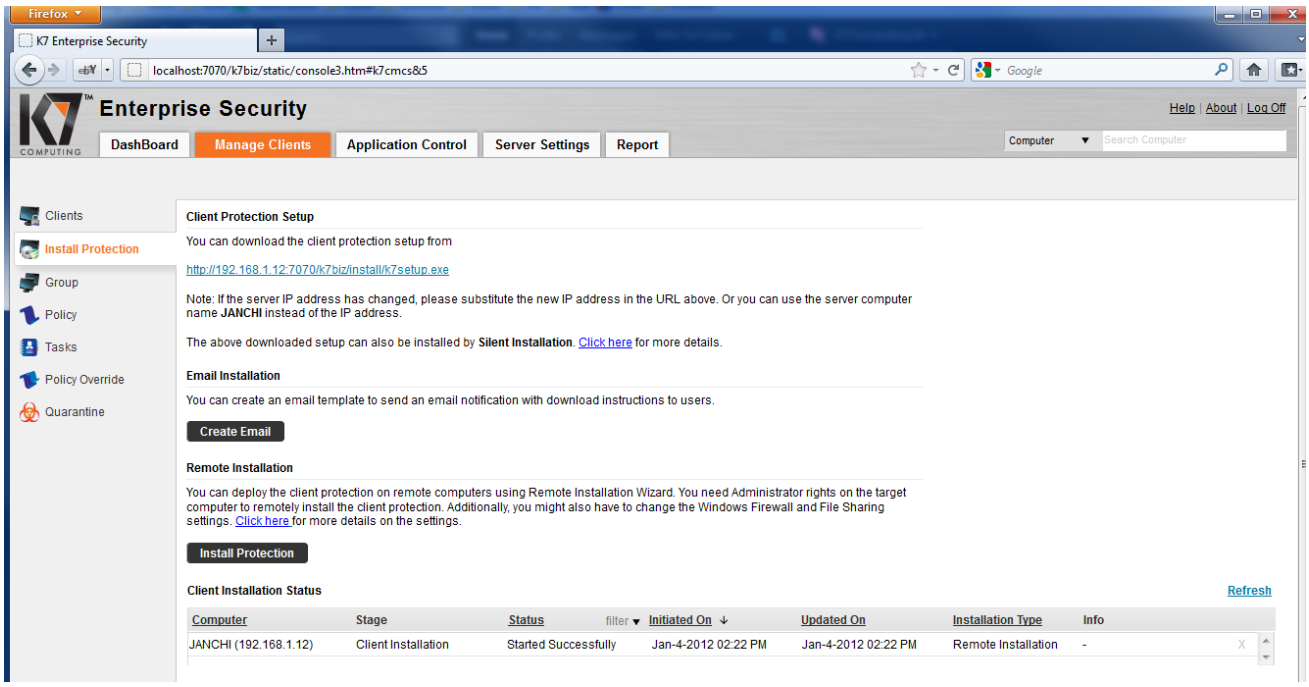
INSTALLING K7 ENDPOINT SECURITY ON CLIENT MACHINES

After installing and activating the server component, you can install K7 protection on client systems *(Manage Clients – Install Protection)* using any of the following methods:

1. **Remote Installation** – You can remotely install K7 Endpoint Security to multiple computers simultaneously from the Admin console. This installation will be done silently without any user interference on the client side.

2. **URL Installation** – You can deploy K7 Endpoint Security by instructing clients to download the setup file from the URL created in the Admin console after the initial installation.

3. **Email Notification** – You can send an email notification to all clients where you wish to install K7 Endpoint Security, URL of the installation file will be automatically added to your email.



Note: K7 End-point security if **installed on MS Server System**, we recommend to disable Firewall protection immediately after installation. Firewall protection in the product it's intended to be used on the end-points but not the server operating systems. To disable the firewall on the server create custom Group - called for example Server, and add your Server client in to this group. Then create custom Policy where you disable Firewall and assign it to the Server Group. This will disable Firewall protection on the Server. More about Policies and Groups bellow.

REMOTE INSTALLATION

Deploying K7 Protection on Client computers is a simple process. You can deploy the client protection on remote computers using Remote Installation Wizard. You need Administrator rights on the target computer to remotely install the client protection.

NOTE: If you want to use the Remote Installation feature – rather than E-mail or URL file installation be aware that Firewall and Windows settings may prevent this.

You might have to change Windows Firewall and File Sharing settings as described below:

Windows XP and Windows 2003 Server

1. Disable 'Simple File Sharing'

To disable 'Simple File Sharing'

1. Go to **My Computer** ➔ **Tools** ➔ **Folder Options** and click the **View** tab
2. In **Advanced Settings** unmark **Use simple file sharing** and click **OK**

2. If Windows Firewall is enabled, allow 'File & Printer Sharing'

To enable 'File & Printer Sharing':

1. Go to **Windows Firewall Exceptions** tab
2. Select **File and Printer Sharing** and click OK

Windows Vista and Windows 2008 Server

If Windows Firewall is enabled, allow 'File Sharing'.

To enable 'File Sharing':

1. Go to **Control Panel** ➔ **Network and Internet** ➔ **Network and Sharing Center**
2. Under **Sharing and Discovery**, select **Turn on file sharing**, and click ***Save Changes***

Windows 7 and Windows 2008 R2

If Windows Firewall is enabled, allow 'File and Printer Sharing'.

To enable 'File Sharing':

1. Go to **Control Panel** ➔ **Network and Internet** ➔ **Network and Sharing Center**
2. Under **File and Printer Sharing** select **Turn on file sharing** and click **Save Changes**

If you don't have Built-in Domain Administrator access, you have to change UAC remote restriction setting on the target computer. (This is not required on Windows XP)

To disable UAC remote restrictions, follow these steps:

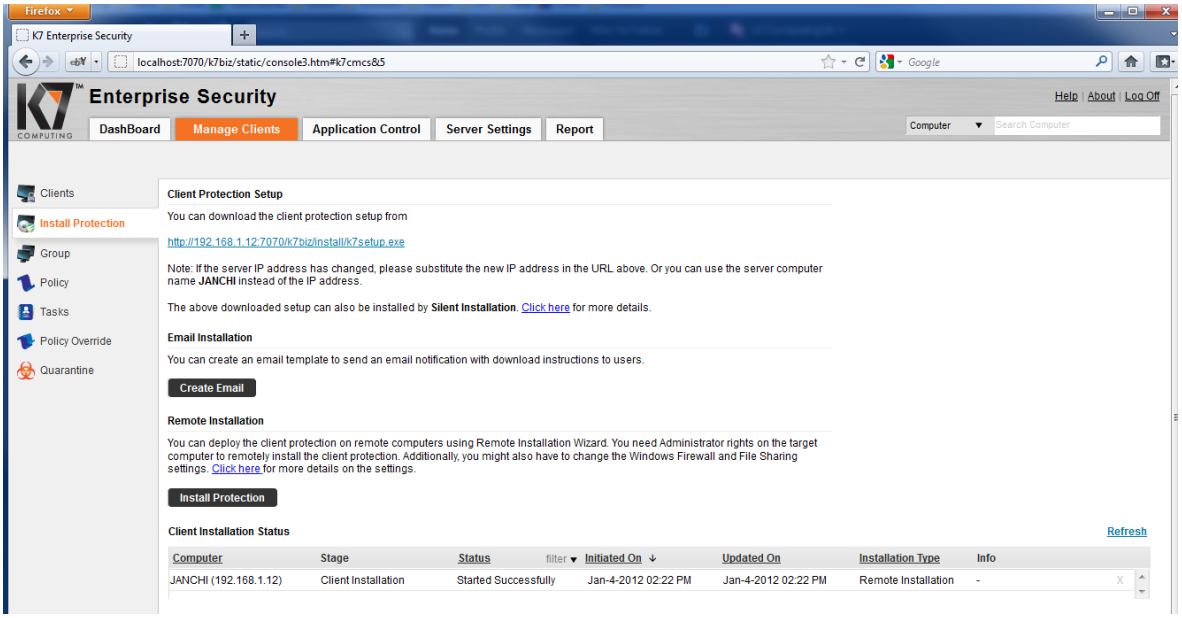
1. Open Windows Registry Editor and locate the following registry sub key:
   KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
2. If the LocalAccountTokenFilterPolicy entry does not exist on the right side, create a **DWORD** named **LocalAccountTokenFilterPolicy** and set **Value Data** to **1**

It is important to have the access to the administrative share of a client computer. This can be verified by running the command: \\NetworkComputerName\C$ **from Run prompt.**

INSTALLING PROTECTION REMOTELY

Once you completed the above client preparation steps, deploying K7 Endpoint Security on client computers is a simple process.

1. Click on the **Install Protection** button to open the remote installation wizard.
2. Specify the Computer Name or IP Address of the system where you want to install K7 Endpoint Security or select **Search Computer** in the **Network** option.
3. Provide the user name and password for selected computers.
4. Specify the Group you wish assign to selected computers and choose the installation option
5. Click Finish



REMOTE INSTALLATION STATUS

You can check the status of the client installations from the **Remote Install Status** table. The following information is shown in Install Status:

- Computer Name / IP Address
- Install Stage (Remote push, installation, 3rd party removal, already installed, etc.)
- Install Status (Initiated, Dispatched, Failed, started successfully, reboot pending by user, completed successfully, etc.)
- Initiated date and time
- Updated date and time
- Failure information

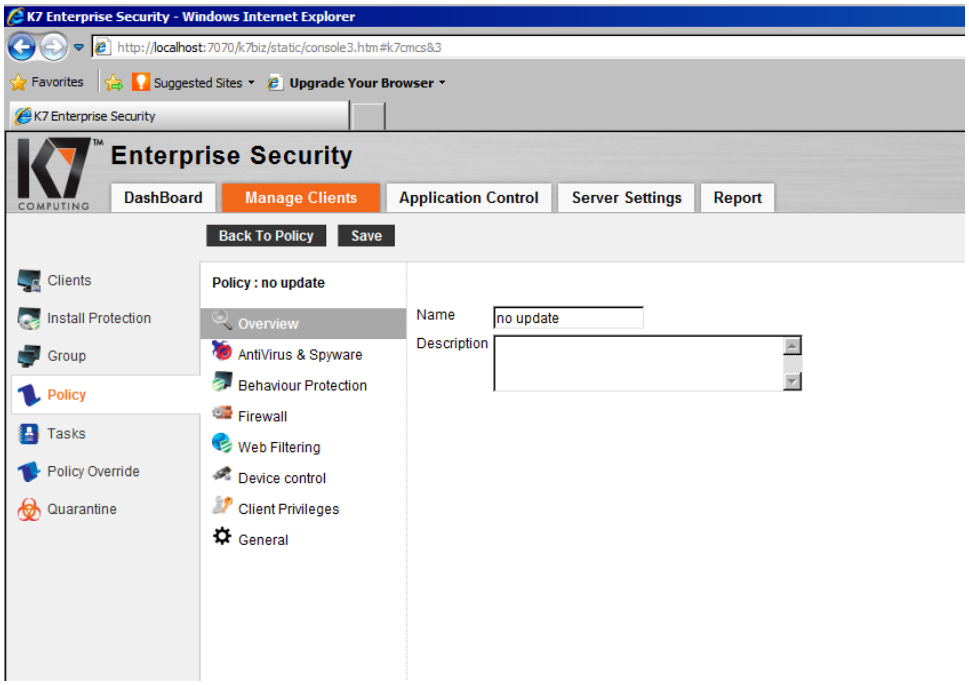
POLICIES

Policies are customized security settings to manage computers on the network. You can use different policies to manage your computers and network security.

Default policy is always created during the initial installation. You can apply this default policy to computers or you can create your own policies to suit your specific security needs. Once the policy is defined it can be assigned to client computers(s) or group(s).

The policies you created are listed under **Policy** and display the following information:

- Name of the Policy
- Description of the Policy
- Number of computers the policy is assigned to
- Policy ID
- Policy created date and time
- Recently modified date and time



You can always create a new policy with defined security settings. You can also edit, copy, or remove the policy, based on the selected policy.
If there are no custom policies created, K7 Default Policy is applied automatically to all client computers.

DEFAULT POLICY

A Default Policy with default factory settings is shipped with the product. The default policy is automatically applied to a computer group if the group does not have an assigned custom policy. Whenever a new client or group is added, this policy will be set as the default policy unless otherwise specified any specific custom policy. K7 Default Policy cannot be edited or removed, however it can be viewed or copied to create a new policy.

HOW TO CREATE A NEW POLICY

You can add a shared policy in the **Policies** page. Locations as well as groups can share the same policy. You must assign the shared policy after you finish adding it.

To create a policy select the **Manage Clients** tab in the admin console and choose **Policy** from the options on the main pane and click **Create Policy.** This will give you a list of options:

1. **Overview** – type in the name of the policy you are about to create and a short description
2. **Antivirus and Spyware** – adjust scanning options and preferences
3. **Behaviour Protection** – enable/disable Browser Protection, Exploits Protection and HIPS
4. **Firewall –** setup In Office and Out Office firewall preferences
5. **Web Filtering** – enable / disable Web Filtering, block websites based on categories and setup Exceptions.
6. **Device Control** – setup preferences for Floppy, Optical and Removable Drives
7. **Client Privileges –** define how users can interact with K7 Endpoint Security
8. **General –** enable / disable automatic updates and notifications on client machines

After you are done editing your policy click **Save** then click **OK** on the dialog box that appears announcing the addition of new Policy.

HOW TO EDIT A POLICY

You can edit an existing policy from the Policy page.

1. Select the **Manage Clients** tab in the admin console and choose **Policy** from the options on the left pane.
2. A list of existing policies will be displayed on the main pane. Choose the policy you wish to edit and click on the **Edit** button. (Please note, you cannot edit the Default Policy)
3. Make the desired changes, click **Save** and **OK** on the dialog box announcing your policy has been updated

HOW TO DELETE A POLICY

You can delete an existing policy from the Policy page.

1. Select the **Manage Clients** tab in the admin console and choose **Policy** from the options on the left pane.
2. A list of existing policies will be displayed on the main pane. Choose the policy you wish to delete and click **Delete**.
3. Click **OK** to confirm deletion.
4. If the selected policy has been assigned to one or more computers, you will receive a warning message asking you if you want to assign the K7 Default Policy after deleting the current policy. Click **OK** to delete the policy and apply the K7 Default Policy to affected computers. Click **Cancel** to cancel deletion. (Please note, you cannot delete Default Policy.)

HOW TO COPY AN EXISTING POLICY TO CREATE A NEW POLICY

Instead of adding a new policy, you may want to copy an existing policy to use as the basis for the new one.

1. Select the **Manage Clients** tab in the admin console and choose **Policy** from the options on the left pane.
2. A list of existing policies will be displayed on the main pane. Choose the policy you wish to copy and click **Copy.**
3. Follow steps 1 – 8 from "HOW TO CREATE A NEW POLICY" to adjust your settings.
4. Click **Save** to save the new policy.

GROUPS

A Group is an organized collection of client computers in the network with similar security needs. You can manage a group of computers as a single unit based on their roles and usage.

For example, you can create groups for departments such as marketing, accounts, engineering, sales and finance, which means each department would get different security and usage levels.

If you have a large network across several locations, you may choose to group computers based on location / department / security level needed.

Clients must be associated with a Group. By default, all client nodes belong to the Default Group. This group cannot be modified or removed.

HOW TO ADD A NEW GROUP

You can add any number of new groups after you define clients with similar security needs.

To add a new group:

1. Select the **Manage Clients** tab in the admin console and choose **Group** from the options on the left pane.
2. Click **Create Group** and specify the name and description of the new group.
3. A list of existing policies will be displayed in the **Select Policy** drop down box. Choose a policy you wish to apply to the new group and click **Add**.
4. Click **OK** on the dialog box announcing the addition of a new group.

Group names may be 255 characters in length and may contain any character except some special characters e.g. [: " / \ * ? < > |]

Group descriptions are not restricted.

HOW TO EDIT A GROUP

You can edit the name of the group and assign a different policy to the group.

1. Select the **Manage Clients** tab in the admin console and choose **Group** from the options on the left pane.
2. Select the group you wish to edit and click **Edit.**
3. You can change the name or description of the group and / or change the policy you wish to assign to this group.
4. Click **Update** when you are done and click **OK** on the dialog box confirming the change.

HOW TO DELETE A GROUP

You can delete any group other than the Default Group. You can however delete a custom group that is marked as the Default Group. If any of the client systems belong to the group you are about to delete, they will be assigned to the Default Group.

1. Select the **Manage Clients** tab in the admin console and choose **Group** from the options on the left pane.
2. Select the group you wish to delete and click **Delete**.
3. Click **OK** to confirm deletion.
4. If one or more clients belong to the group you are about to delete, a warning message will be displayed asking you to assign effected client(s) to the Default Group. Click **OK** to proceed. Click **Cancel** to cancel the deletion.

HOW TO MARK A GROUP AS THE DEFAULT GROUP

You may mark any custom group as the Default Group. This way, whenever a new client system is added, it will be assigned by default to the Default Group unless otherwise specified.

1. Select the **Manage Clients** tab in the admin console and choose **Group** from the options on the left pane.
2. The drop-down menu next to **Default Group** lists all the groups that are currently available. Select a group to be set as the default group.
3. Whenever a new client system is added, it will be assigned to this group.

CHANGE GROUP

You can also change the group for one or more computers from here. To change the group for more clients:

1. Click on the **Change Group** button, this will navigate you to the Change Group dialog.
2. Select a group from the drop-down menu and click the **Show** button to view computers associated with the selected group.
3. From the listed client list select the computers you wish to move another group and click **Add**
4. Click **Next** to view the **Group list** and assign a new group to selected computers.
5. Click **Finish**

MANAGE CLIENTS

You can view a list of client machines in the admin console where K7 Endpoint Protection was already installed and the security status of respected clients in the Clients view. The following information is visible:

- Computer Name
- Group
- Antivirus and Firewall Status
- Endpoint Security Version
- Virus definition version
- Last updated date and time

You may also select **Filter** to view a list of computers based on filter criteria. You can select any of the following filter categories:

- Group
- Update Status
- Protection Status
- Operating Systems of client machines
- Client machines that are not scanned
- Client machines are that are not communicating with the server
- IP Address

When you click on a client machine, it gives you a detailed view of that particular computer. You can view the following information in **Computer Overview**:

- Computer Name
- IP Address
- Operating System
- Assigned Group
- Policy associated with assigned Group
- Date and time of installation
- Last Contacted Date and time
- Virus Detection information
- Protection Status
- Applications accessed
- Detected threats information

Managing groups and policies can be easily done using the **Manage Clients** where you can perform the following:

- Install K7 Endpoint Security on client machines
- Manage Groups – Create / Edit / Delete Groups
- Manage Policies – Create / Edit / Copy / Delete Policies
- Manage Tasks for individual computers or groups
- Policy Override Settings
- Quarantine Settings

MANAGING TASKS

In addition to the Real Time protection available in K7 Endpoint Security, as an administrator you can specify on-demand/scheduled scans to run on client systems. You can create a new task and specify the system / group to which it has to be assigned. You can view the status of the task and even remove tasks.

You can choose any of the following Scan types or Updates when creating a new task.

- **Quick Scan** – Scans important drives and folders (C:\ drive, Windows Folders and Program Files) on client machines.
- **Complete Scan** – Scans the entire system including all files, folders and drives
- **Rootkit Scan** – detects and removes rootkits from the endpoints
- **Vulnerability Scan** – detects vulnerable application modules and informs the administrator about potential risks
- **Tracking cookie** – finds and removes tracking cookies from endpoints
- **Custom Scan** – allows the administrator to customize scan tasks e.g. location, file types, action taken
- **Update** – runs an update on selected endpoint

FILTER TASKS STATUS

Administrator can filter tasks from the list of existing tasks displayed based on the following criteria:

- **Pending** – tasks still running
- **Dispatched** – tasks initiated on client machines
- **Completed** – tasks successfully completed

REMOVING A TASK

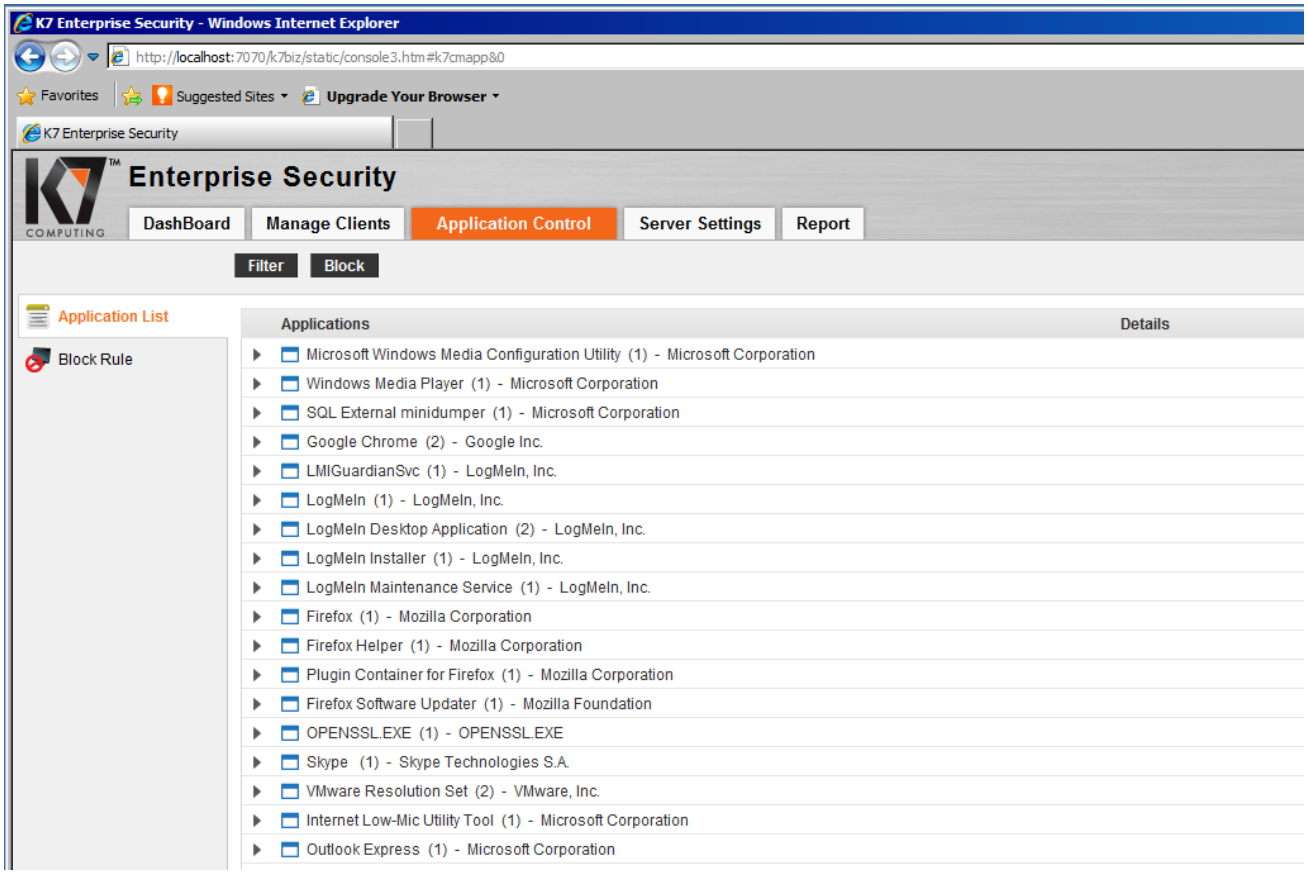
A list of existing tasks is displayed on the Manage Tasks page. Select a task you wish to remove and click on the Delete button.

APPLICATION CONTROL

Application control's objectives relate to security, integrity and availability of applications only for intended users. Administrators can implement restrictions and control unwanted applications clogging the network on client machines by using **Application Control**. This feature effectively addresses security concerns caused by applications as instant messengers, download managers, Bit-torrent clients, etc.

Application Control can perform the following tasks:

- block an application from running
- block an application from connecting to the Internet
- block complete network access for an application



VIEWING THE APPLICATION LIST

Application control is implemented by a set of rules that define whether the applications you specify can be executed or connected to the internet or connected to the network. A list of applications is available on the Applications List page. You can also search for applications on a specific computers or by using the software publisher's name.

You can filter applications based on the following criteria:

- Application Type
- Application Name
- Computer Name
- MD5
- Access Type
- Publisher
- Reported Date

BLOCKING AN APPLICATION FROM THE APPLICATION LIST PAGE

You can search for an application based on publisher, computer or other filter parameter. The selected application(s) can be blocked on a single machine, multiple computers in a group or across groups.

APPLICATION BLOCK RULE

This feature allows Administrators to block applications based on the application's name or file hash (MD5). The application block rule can be applied to a single computer, multiple computers in a group or across the groups. This feature offers flexibility to Network Administrators on what applications to block and enables them to meet security and productivity concerns that result from uncontrolled use of applications across the organization.

The options available to impose access restrictions are:

- Block Application from running
- Block Internet Access for the Application
- Block Network Access for the Application

POLICY OVERRIDE

If you need to apply any configuration or settings across all client machines, you can do so by using **Policy Override** without having to change all the policies. Administrators can use this feature to enforce a blanket rule / restriction across all computers easily.

Policy override offers two ways for the policy change:

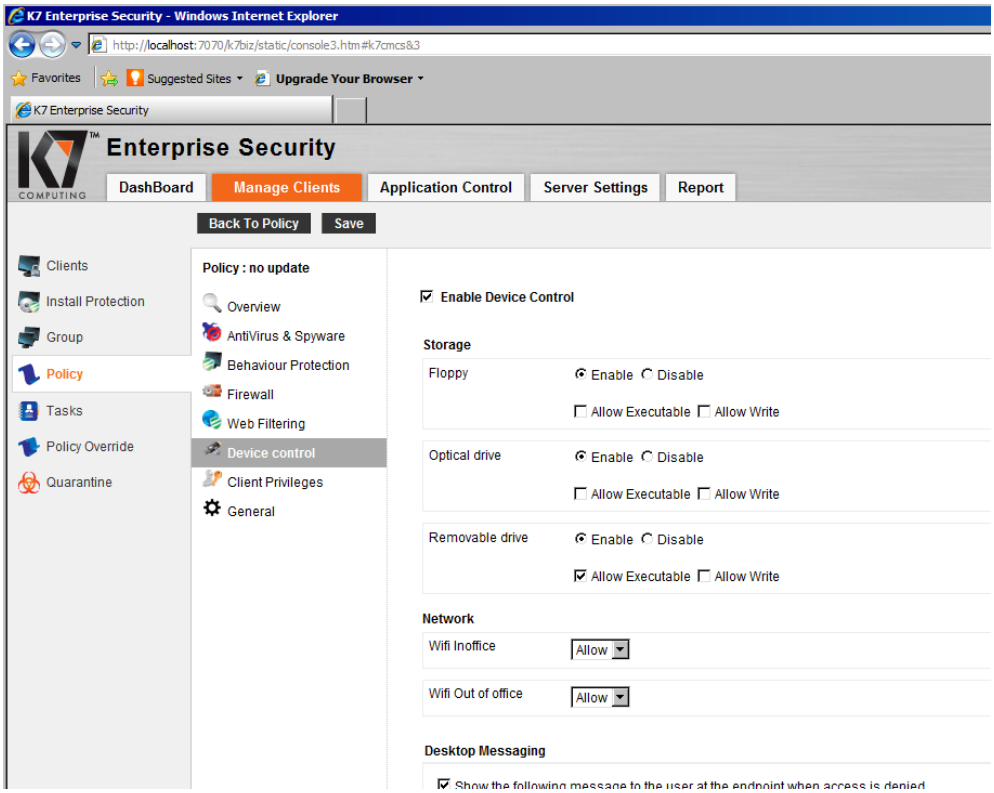
1. Override: This type of configurations supersedes the policy settings.
e.g. Disabling Removable Drives on all computers overriding the policy settings.

2. Extended Settings: This type of override enables you to specify settings in addition to what is provided in the policies. e.g. Blocking certain websites on all computers in addition to the blocked websites already setup in policies.

Override can be applied to: Scan, Device Control, Internet Access, and Firewall and **it is executed immediately on endpoints.**

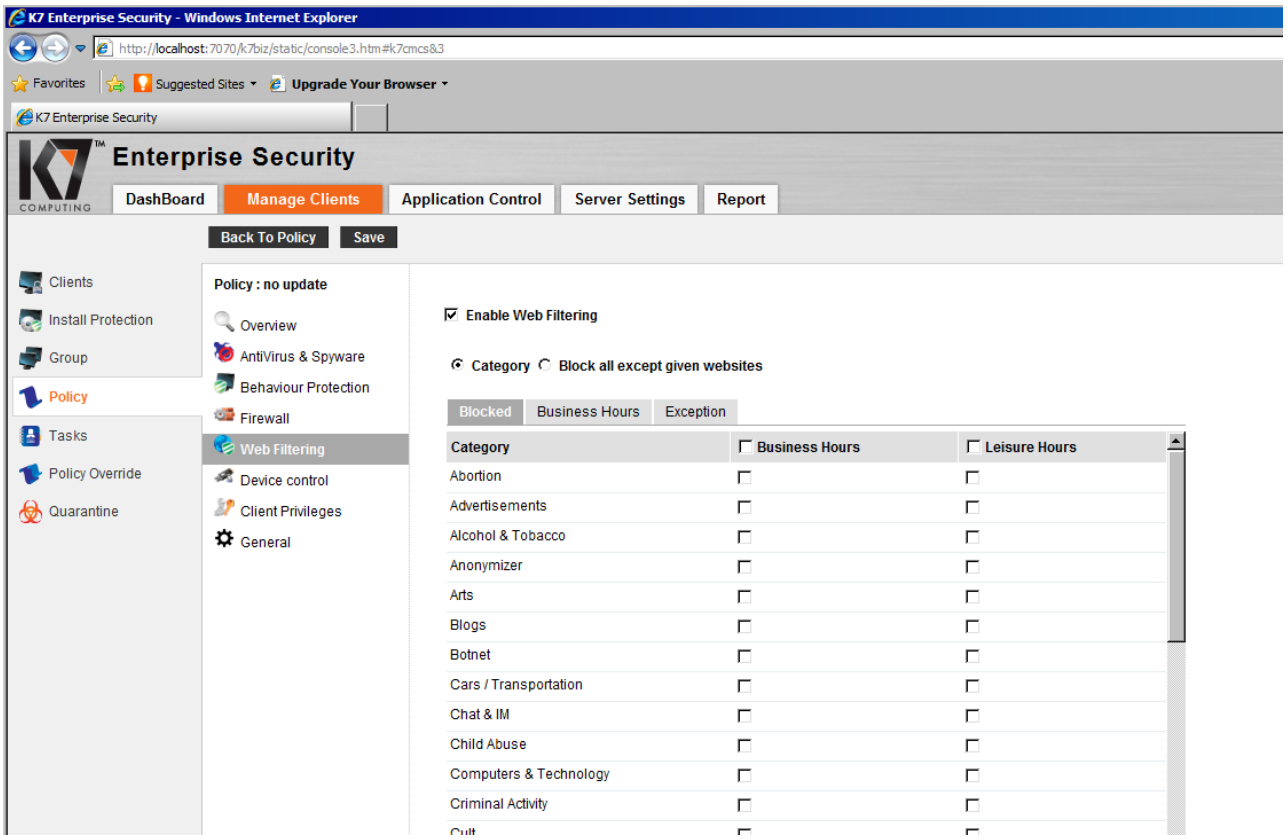
REMOVABLE DRIVES

You can easily block Removable Drives under Policy Override. You don't need to change Device Control settings in all the policies. Or you can apply the rule in the policy specific for each group of clients:


K7 Enterprise Security - Windows Internet Explorer
http://localhost:7070/k7biz/static/console3.htm#k7cmcs&3
Favorites
Suggested Sites
Upgrade Your Browser
K7 Enterprise Security
Enterprise Security
DashBoard
Manage Clients
Application Control
Server Settings
Report
Back To Policy
Save
Clients
Install Protection
Group
Policy
Tasks
Policy Override
Quarantine
Policy : no update
Overview
AntiVirus & Spyware
Behaviour Protection
Firewall
Web Filtering
Device control
Client Privileges
General
Enable Device Control
Storage
Floppy
Enable
Disable
Allow Executable
Allow Write
Optical drive
Enable
Disable
Allow Executable
Allow Write
Removable drive
Enable
Disable
Allow Executable
Allow Write
Network
Wifi Inoffice
Allow
Wifi Out of office
Allow
Desktop Messaging
Show the following message to the user at the endpoint when access is denied

WEB FILTERING

The Web Filtering option allows administrators to specify website types to be blocked based on pre-defined rules: e.g. Gambling, Social networks, Chats, etc. and to enforce these rules based on time schedules. Different types of web filtering rules can be setup for Business and Leisure hours.



OTHER FEATURES:

CLIENT'S DIRECT FUNCTIONS:

To see the options for direct client management right-mouse click on the client's name in the Client List and a full menu of executable options will show up. This will allow you to send new Tasks, Scan, Restart, Update, and Changes Group instantly.

REPORTS

The Report feature within K7 Enterprise security is providing detailed reports on network status based on constantly updating logs.
Some of the reports available are: Most Common Threats, Top Websites Blocked, Top Applications Blocked, and more. Reports can be fetched at any time for a particular Group within a defined timeframe.

SERVER SETTINGS

Administrator – contains login information of the administrator and login times. You can change the Administrator password here

Notification – setup SMTP for e-mail notifications sent to administrators/managers with custom options on report types

Location Detection – set rule for in / and out of network settings that will be further applied to clients for out-of-office policies

Proxy Settings – change if your network is using proxy

Licence – detailed licence information