Defenx Network Security

Product Manual

About the Admin Console

The Admin Console is a centralized web-based management console. The web console is accessible through any modern web browser from any computer on the network and you can manage the entire security settings including installing clients, managing Groups, Policies, Tasks, Updates, Antivirus, Firewall, Application Control, Web Filtering, Notifications etc.

Dashboard

Dashboard is the main console where the administrator can have the easy and quick glimpse of the Defenx Endpoint – Client products security status such as 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, Subscription, etc. If anything is unusual in the dashboard status then Administrator can quickly navigate to the problem by clicking on the corresponding issue link on the widget which will show the detailed report of the status.

Installing Defenx Endpoint Security on Clients

After installing and activating the server component, you can install the Defenx protection on client systems using any one of the following methods.

1. Remote Installation – You can remotely install the Defenx Protection to multiple computers simultaneously from the Admin console. This installation will be done silently without any user interface involvement

2. URL Installation – You can deploy the Defenx Protection to clients by instructing end users to download the setup file from the URL which is specified in the Admin console.

3. Email Notification – You can send an email notification to all users on whose systems you wish to install the Defenx Client Protection by specifying the download URL of the client setup file.

Remote Installation

Deploying Defenx 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. Additionally, you might also have to change the Windows Firewall and File Sharing settings which have been described below:

Windows XP and Windows 2003 Server

1. Disable 'Simple File Sharing'

   To disable simple file sharing,

   i. Go to **My Computer** → **Tools** menu → **Folder Options** and click the **View** tab

ii. In the **Advanced Settings** section, clear the **Use simple file sharing** and click **OK**

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

To enable 'File & Printer Sharing', follow these steps:

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, then allow 'File Sharing'.

To enable 'File Sharing',

i. Go to **Control Panel → Network and Internet → Network and Sharing Center**

ii. Under **Sharing and Discovery**, select **Turn on file sharing**, and click **Save Changes**

Windows7 and Windows 2008 R2

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

To enable 'File Sharing',

iii. Go to **Control Panel → Network and Internet → Network and Sharing Center → Change Advanced Sharing Settings**

iv. Under **File and Printer Sharing** select **Turn on file sharing** and click **Save Changes**

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

To disable UAC remote restrictions, follow these steps:

1. Open Windows Registry Editor and locate the following registry subkey: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
2. If the LocalAccountTokenFilterPolicy entry does not exist in the right side, create a **DWORD** name as **LocalAccountTokenFilterPolicy** and enter the **Value Data** as **1**

Importantly you need 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 with the above client preparation steps, deploying Defenx Protection 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 on which you want to install the Client Protection or select the Search Computer on Network option.

3. Provide the user name and password for the selected computers

4. Specify the Group that you wish to apply to the 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 are 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 the computers which are in the network. You can use different policies to manage your computers' and network security.

A default policy is created always 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 Computer(s) or Group(s).

The policies you created are listed under **Policy** page and show the following information as well:

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

You can always create a new policy with defined security settings. Moreover you can edit, copy, or remove the policy, based on the selected policy.

When no custom policies are created, the Defenx Default Policy is applied to all the 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. The Defenx 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.

1. Select **Manage Clients** tab on the admin console and choose **Policy** from the options on the left pane.
2. Click **Create Policy.** Various sections like **Overview**, **AntiVirus and Spyware** etc appear on the left pane. Type in a suitable name and description of the policy on the **Overview** page.
3. Choose the **AntiVirus and Spyware** option from the left pane and select/unselect the desired options from the four tabs that appear on the main pane.
4. Select **Behavior Protection** from the left pane and select/unselect the desired options to be applied.
5. Choose the **Firewall** option on the left pane and select the desired **In Office** and **Out Office** settings.
6. Choose **Web Filtering** and select the desired options on the three tabs, **Filter, Business Hours** and **Exceptions** that appear on the main pane.
7. Choose **Device Control** and select the desired options on the main pane.
8. Click **Save** and click **OK** on the dialog box that appears announcing the addition of the new policy.

How to edit a policy

You can edit an existing policy from the Policy page.

1. Select **Manage Clients** tab on the admin console and choose **Policy** from the options on the left pane.
2. A list of existing policies is displayed on the main pane. Choose the policy you wish to edit and click on **Edit** button. (Please note, you cannot edit Default Policy)
3. Make the desired changes on various sections like **AntiVirus and Spyware, Behavior protection,** etc. that are displayed on the left pane.
4. When you're done, click **Save** and click **OK** on the dialog box that appears announcing that the policy has been updated.

How to delete a policy

You can delete an existing policy from the **Policy** page.

1. Select **Manage Clients** tab on the admin console and choose **Policy** from the options on the left pane.
2. A list of existing policies is displayed on the main pane. Choose the policy you wish to delete and click on **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 that asks you if you want to assign the Defenx Default policy after deleting the current policy. Click **OK** to delete the policy and apply the Defenx Default Policy to the 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 policy.

1. Select **Manage Clients** tab on the admin console and choose **Policy** from the options on the left pane.
2. A list of existing policies is displayed on the main pane. Choose the policy you wish to copy and click on **Copy Policy**.
5. Provide an appropriate name and description for the new policy and make the desired additions/changes to the policy by selecting various sections like **AntiVirus and Spyware, Behavior protection,** etc. that are displayed on the left pane.
3. 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 similar security and usage levels.

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

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

How to add a new group

You can add any number of new groups after you define the similar computers of your organization. To add a new group

1. Select **Manage Clients** tab on the admin console and choose **Group** from the options on the left pane.
2. Click on **Create Group** and specify the name and description for the new group.
3. A list of existing policies is displayed in the Select Policy drop down box. Choose a policy that 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 it may contain any character except some special characters such as [: " / \ * ? < > |]

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 **Manage Clients** tab on the admin console and choose **Group** from the options on the left pane.
2. Select the group you wish to edit and click on **Edit.**
3. You may specify a new name or description for the group and/or change the policy that you wish to assign to the group.
4. Click **Update** when you're done and click **OK** on the dialog box confirming the change.

How to delete a group

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

1. Select **Manage Clients** tab on the admin console and choose **Group** from the options on the left pane.
2. Select the group you wish to delete and click on **Delete**.
3. Click **OK** to confirm deletion.
4. If one or more systems belong to the group you want to delete, a warning message appears asking you if you want to assign those computers to the Defenx 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 is, by default, assigned to the Default Group unless otherwise specified.

1. Select **Manage Clients** tab on the admin console and choose **Group** from the options on the left pane.
2. The drop-down button 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.

Manage Clients

From the Admin console, you can view the list of client computers on which Defenx Protection has been installed and the security status of the respective clients from the Clients view. It gives the following information to the administrator:

- 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 the particular list of computers based on filter criteria. You can select any of the following filter categories:

- Group
- Update Status
- Protection Status
- Operating Systems of the Client Computers
- Computers which are not scanned
- Computers which are not communicated with server
- IP Address

When you click on a particular computer's name it gives a 360 view about the particular computer. You can view the following information from Computer 360:

- Computer Name
- IP Address
- Operating System
- Group

- Policy
- Installed Date and time
- Last Contacted Date and time
- Virus Detection information
- Protection Status
- Applications accessed
- Detected threats information

Moreover managing groups, policies etc. can be done easily with the Manage Clients tab and from the left pane under 'Manage Clients' you can perform the following:

- Install Endpoint Security on clients
- 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

Change Group

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

1. Click on **Change Group** button and you will get Change Group dialog.
2. Select a group from the listed drop down box and click **Show** button to view computers associated with the selected group.
3. From the listed computers list select the computers that you want to move other group, and click **Add**
4. Now Click next to view the Group list which you have already and choose a new group for the selected computers.
5. Click **Finish**

Managing Tasks

In addition to the Real Time protection available in Defenx clients, 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 one of the following Scans or Update to create a new task.

- Quick Scan
- Complete Scan
- Rootkit Scan
- Vulnerability Scan
- Tracking cookie
- Custom Scan
- Update

Adding a new Task

You can choose any one of the following scans to create a new task.

Quick Scan – Scans important drives and folders (C drive, Windows folder and Program Files folder) on your system for viruses and other potential threats.

Complete Scan – Scans your entire system including all files and folders and drives

Rootkit Scan – This option can be used to scan the system generically for rootkits.

Vulnerability Scan – Scans and informs the users about vulnerabilities in the system.

Tracking cookie – Tracking cookies are bits of information stored on a system by a browser which enable a website to uniquely identify a user. The scan for Tracking cookies sans for tracking cookies present in the currently logged in user.

Custom Scan – Allows you to customize your scan task. You can choose the locations to scan, file types to scan and decide on the action to take if a malware is found.

Filter Tasks Status

From the list of existing tasks displayed, you can filter the tasks according to the following status:

- Pending – Task which is still running
- Dispatched – Which has been initiated on client computer
- Completed – The task which has been completed successfully on the client system

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 objectives relate to security, integrity and availability of applications only to intended users. Using Application Control, you can implement restrictions on application usage in client computers. Network Administrators will be able to control unwanted applications that clog the network. This feature effectively addresses security concerns caused by some applications such as instant messengers, download managers, etc.

Using Application control,

- You can block an application from running
- You can block an application from connecting to the Internet
- You can 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 computer or by Publisher's name.

You can also filter the applications based on the following parameters

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

Blocking an Application from the Application List page

You can search for applications based on Publisher/Computer or filter parameters and the selected application(s) can be blocked on a single computer or multiple computers in a group or across the groups.

Application Block Rule

This feature allows Administrators to block applications based on the application name or file hash (MD5). The application block rule can be applied to a single computer or 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/settings across the computers, you can achieve it 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 types configuration overrides.

1) Override: The override configuration supercedes all the policy settings. E.g. you have not setup any restrictions on Removable Drive in your policies. Later on, the need arises to block the Removable Drive access on the all the computers. You can easily block the Removable Drive under Policy Override. You don't need to change the Device Control settings in all the policies.

2) Extended Settings: This type of override enables you to specify settings in addition to what is provided in the policies. E.g. you have already setup Web Filtering in all your policies. Now you need to block certain websites across the computers. The additional websites can easily be blocked under Policy Override. You don't need to add these websites under each policy.

You can use this feature to enforce Scan options, Firewall settings, Device Control, list of Allowed Websites and Blocked Websites, In Office and Out Office Security settings and Global File Exclusion list.