



www.cornerpost.net

Internet Management Products

1. Configuring a Chaperon Policy
 - a. Editing the Existing “Default Installation Policy”
 - b. Creating a New Policy
2. Managing User-Defined Filters
 - a. Creating a new User-Defined Deny List to Block Additional Websites
 - b. Creating a new User-Defined Allow list to Unblock Websites Filtered by Chaperon
 - c. Activating a User-Defined List
 - d. Importing and Exporting User-Defined Lists
 - i. Exporting a User-Defined List
 - ii. Importing a User-Defined List
3. Configuring Chaperon Notifications
 - a. Configuring SMTP Server Settings
 - b. Configuring Notification Recipients
 - i. Editing the Default Notification Recipient
 - ii. Adding New Notification Recipients
 - iii. Setting Notification Recipients Based on Active Directory User Managers
 - c. Setting What Chaperon Categories to Receive Notifications For
4. Setting Chaperon Category Redirect Pages
5. Configuring the Filter Update Schedule
6. Entering Your Registration Key
7. Things to Remember

Revised November 02, 2006

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

1. Configuring a Chaperon Policy

A Chaperon policy is used to specify what sites will be filtered, the content on those sites that will be filtered, the schedule the filtering will occur, and to whom the filtering will apply. Chaperon can be configured for multiple policies based on these items.

Note: The Users, Networks, Computers, Subnets, Address Ranges, Schedules, and Content types that are available for use in Chaperon policies are all objects contained within ISA Server. As such, any new entries for each of these objects will need to be created in ISA server first, followed by applying the changes. Any new entries created will be available for use once the Chaperon Control Panel is refreshed (By using the refresh image on the Policies tab), or when the Chaperon Control Panel is closed and reopened. Refer to ISA documentation for instructions for creation of any of the aforementioned objects.

1.a Editing the Existing “Default Installation Policy”

Chaperon comes pre-configured with a default installation policy. This basic policy applies to “All Users” and has the basic Chaperon categories selected. This policy can be used as-is, or it can be configured to meet your needs more closely which is recommended. The following steps explain editing the default policy.

1. In the Chaperon Control Panel, click the Policies tab.
2. In the policy list on the left, click on “Default Installation Policy Permanent” to highlight it for editing.
3. In the “Policy Name” section, the policy can be renamed or left as is.
4. In the users section, “All Users” will be selected. This can be changed to any specific users that are specified within ISA.
 - If all users on your network will have the same filtering policy, this setting is recommend left as the default “All Users”.
 - If specific users or groups are to be specified, “All Users” will need to be unchecked or there will be no change in filtering.
 - **Important:** If specific users or groups are specified within a Chaperon policy, but the allow rule in ISA applies to “All Users”, the Chaperon policy will not work. This is due to ISA not requiring authentication from the users, which causes the request to be received as the “anonymous” user. Since the Chaperon rules would apply to a specific user or group and not “anonymous”, the filtering would not apply to that traffic. This is corrected by editing your ISA allow rule by removing “All Users” and adding the correct users or groups. The “Domain Users” group works well for this if all users in the domain are to have Internet access. Keep in mind that setting the allow rule in this fashion will deny all anonymous access. So any servers or non-windows machines will need to have a separate rule created to allow them access by IP address that is placed above the rule applied to specific users.
5. The “Applies to Traffic From” tab specifies the origin of traffic the policy will apply to. Networks, Computers, Subnets, and Address Ranges can be specified. The default setting will be appropriate in most cases. Exceptions in these sections need only be configured if they are contained within an entry in the Include section. For instance, adding an exception for a Computer specified in

- “Computers”, because it’s IP is contained within an Address Range that is specified would be correct.
6. On the Schedule tab under weekly schedule, select the schedule to be used for this policy. The default is “Always”.
 7. On the Schedule tab under “Effective Dates”, specific date ranges can be set for policies to be active. “Permanent” is the default and is recommended.
 8. The categories tab shows all Chaperon categories and all user-defined allow and deny lists. Select the categories that will apply to this policy. The “All External Traffic” box will apply to all traffic and is normally only used in conjunction with specific content types, which are explained next.
 - **Important:** If “All External Traffic” is checked and the content types are left to the default, all traffic will be blocked.
 9. On the “Content Types” tab, the types of content to be blocked from the sites that are specified on the categories tab can be configured. To block the entire site, “All Content Types” should be checked. To block only a certain content type in the list, uncheck the “All Content Types” box and select only the specific types you wish to be blocked.
 - **Important:** If the “All Content Types” box is not checked, and no content types in the list are checked either, then no content on the sites will be blocked, which will essentially allows the site.
 10. Click Save on the Policies tab to save the Changes.

1.b Creating a New Policy

1. In the Chaperon Control Panel, click the Policies tab.
2. On the bottom left, click the New button.
3. In the “Policy Name” section, give the policy a descriptive name.
4. In the users section, “All Users” will be selected. This can be changed to any specific users that are specified within ISA.
 - If all users on your network will have the same filtering policy, this setting is recommend left as the default “All Users”.
 - If specific users or groups are to be specified, “All Users” will need to be unchecked or there will be no change in filtering.
 - **Important:** If specific users or groups are specified within a Chaperon policy, but the allow rule in ISA applies to “All Users”, the Chaperon policy will not work. This is due to ISA not requiring authentication from the users, which causes the request to be received as the “anonymous” user. Since the Chaperon rules would apply to a specific user or group and not “anonymous”, the filtering would not apply to that traffic. This is corrected by editing your ISA allow rule by removing “All Users” and adding the correct users or groups. The “Domain Users” group works well for this if all users in the domain are to have Internet access. Keep in mind that setting the allow rule in this fashion will deny all anonymous access. So any servers or non-windows machines will need to have a separate rule created to allow them access by IP address that is placed above the rule applied to specific users.
5. The “Applies to Traffic From” tab specifies the origin of traffic the policy will apply to. Networks, Computers, Subnets, and Address Ranges can be specified. The default setting will be appropriate in most cases. Exceptions in these sections need only be configured if they are contained within an entry in the Include

- section. For instance, adding an exception for a Computer specified in “Computers”, because it’s IP is contained within an Address Range that is specified would be correct.
6. On the Schedule tab under weekly schedule, select the schedule to be used for this policy. The default is “Always”.
 7. On the Schedule tab under “Effective Dates”, specific date ranges can be set for policies to be active. “Permanent” is the default and is recommended.
 8. The categories tab shows all Chaperon categories and all user-defined allow and deny lists. Select the categories that will apply to this policy. The “All External Traffic” box will apply to all traffic and is normally only used in conjunction with specific content types, which are explained next.
 - **Important:** If “All External Traffic” is checked and the content types are left to the default, all traffic will be blocked.
 9. On the “Content Types” tab, the types of content to be blocked from the sites that are specified on the categories tab can be configured. To block the entire site, “All Content Types” should be checked. To block only a certain content type in the list, uncheck the “All Content Types” box and select only the specific types you wish to be blocked.
 - **Important:** If the “All Content Types” box is not checked, and no content types in the list are checked either, then no content on the sites will be blocked, which will essentially allow access to the sites.
 10. Click Save on the Policies tab to save the Changes.

2. Managing User-Defined Filters

User-Defined filters are what Chaperon uses when a site needs to be unblocked, or additional sites need to be blocked. User-Defined Allow lists are used to unblock sites, while User-Defined Deny lists are used to block sites. Multiple Allow and Deny lists can be created, and each list can hold multiple entries. This allows for sites to be blocked or unblocked for specific users instead of a single unblock or block list for everyone.

2.a Creating a new User-Defined Deny list to block websites

1. In the Chaperon Control Panel, navigate to the “User-Defined Filters” tab.
2. On the bottom left in the Filter section, click the New button.
3. In the “List Name” section, give the list a descriptive name.
4. For “List Type”, select “Deny and Redirect To”.
5. In the box directly to the right of “Deny and Redirect To”, type the URL of where the user will be redirected to when they attempt to visit sites that will be included in this list. URLs that redirect to any type of content can be used, such as redirecting them to a website, or redirecting them to a specific image.
6. In the Comment section, a comment for the list can be entered but is not required.
7. Click the New button in the Entry section to begin adding entries to the list.
8. Select the “Entry Type” to be used for the entry. If blocking a specific website as a whole, select Domain. If blocking a specific IP Address, select IP Address. If blocking a specific path, select URL/Path.
9. Multiple sites can be added to each list. Using the Entry box, enter each entry that is to be blocked followed by using one of the Save buttons. Repeat steps 8

and 9 for each entry. Click “Save and Close” on the last entry, or click the cancel button when all entries have been added.

- **Domain Entry Note:** When blocking an entire domain, two entries must be specified for each site. For instance, if a user wanted to block the domain examplesite.com, one entry would be needed as *.examplesite.com with the other entry being examplesite.com. The first entry *.examplesite.com would block all request such as www.example.com, mail.example.com, etc, while the example.com entry would block requests there were received without a sub domain such as http://examplesite.com.



Entries	
Entry	Type
examplesite.com	Domain
*.examplesite.com	Domain

10. Click Save on the “User-Defined Filters” tab to save the list.
11. The list is now created but will not be in effect until it is added to a policy. Follow the steps in section 2.c (Activating a User-Defined List) for the steps involved in enabling the list.

2.b Creating a new User-Defined Allow list to unblock websites

1. In the Chaperon Control Panel, navigate to the “User-Defined Filters” tab.
2. On the bottom left in the Filter section, click the New button.
3. In the “List Name” section, give the list a descriptive name.
4. For “List Type”, select Allow.
5. In the Comment section, a comment for the list can be entered but is not required.
6. Click the New button in the Entry section to begin adding entries to the list.
7. Select the “Entry Type” to be used for the entry. If blocking a specific website as a whole, select Domain. If blocking a specific IP Address, select IP Address. If blocking a specific path, or a specific file located on a site, select URL/Path.
8. Multiple sites can be added to each list. Using the Entry box, enter each entry that is to be blocked followed by using one of the Save buttons. Repeat steps 8 and 9 for each entry. Click “Save and Close” on the last entry, or click the cancel button when all entries have been added.

- **Domain Entry Note:** When unblocking an entire domain, two entries must be specified for each site. For instance, if a user wanted to unblock the domain examplesite.com, one entry would be needed as *.examplesite.com with the other entry being examplesite.com. The first entry *.examplesite.com would block all request such as www.example.com, mail.example.com, etc, while the example.com entry would block requests there were received without a sub domain such as http://examplesite.com.



Entries	
Entry	Type
examplesite.com	Domain
*.examplesite.com	Domain

9. Click Save on the “User-Defined Filters” tab to save the list.
10. The list is now created but will not be in effect until it is added to a policy. Follow the steps in section 2.c (Activating a User-Defined List) for the steps involved in enabling the list.

2.c Activating a User-Defined List

When a new user-defined allow or deny list is initially created it will not be in effect until it is added to a policy. The new allow or deny list will be available as a new category on Chaperon's policy tab that is named after the user-defined list. If the list is an allow list, the name would be preceded by "UDF-A", while a deny list will be preceded by "UDF-D". For Example, if you created a deny list named "My Deny List", the list would appear as a new Chaperon category on the Policies tab named "UDF-D My Deny List".

The following steps outline adding a recently created list to a policy.

1. In the Chaperon Control Panel, click on the Policies tab.
2. In the policy list, click the policy you wish for the allow or deny list to apply to.
3. Click on the Categories tab.
4. Check the box next to the deny or allow list you wish to use in this policy.
5. Click the Save button.
6. The changes will not take effect until the next filter update. To start a filter update immediately, navigate to the Dashboard tab and click the "Update Filter" link. Once the update is complete, the list will be in effect.

2.d Importing and Exporting User-Defined Lists

Chaperon includes the ability to import and export previously created User-Defined lists. This feature can be utilized in multi Chaperon environments to quickly add an identical User-Defined list to additional Chaperons without having to recreate the lists each time. The lists can simply be exported on one Chaperon, and then the exported file can be imported into a different Chaperon, saving configuration time. These exports can also be used as individual backup copies of the User-Defined lists.

2.i Exporting a User-Defined List

1. Open the Chaperon Control Panel and Navigate to the User-Defined Filters tab.
2. Highlight the filter you wish to export by clicking it.
3. Click the Advanced button.
4. Click the Export tab.
5. Using the Browse button (...) select a directory for the file to be placed, and supply a filename, followed by clicking the Open button.
6. Click the OK button on the Import/Export window to begin the export.
7. When the process is complete, click the Close button.

2.ii Importing a User-Defined List

1. Open the Chaperon Control Panel and Navigate to the User-Defined Filters tab.
2. Click the Advanced button.
3. Click the Import tab.
4. Click the Browse button (...) and locate the file you wish to import, followed by clicking the Open button.
5. Click OK on the Import/Export window to begin the import.
6. When the process completes, click the Close button.

- **Important:** The time it takes for a User-Defined Import and Export to complete will vary depending on the amount of entries in the list. Larger lists will take much longer to Import and Export. During the Import/Export Process, the Import/Export window will not be responsive. The process should not be interrupted, as this activity is normal.

3. Configuring Chaperon Notifications

Chaperon utilizes a notification feature to notify for all user and service activity. There are three basic types of notifications which are outlined below:

- **Chaperon Service Event Notifications** – These notifications are used for Chaperon specific information such as Chaperon service start/stop, software update availability, account expiration, or Chaperon errors. These notifications are only sent to the default notification recipient.
- **Filter Hit Limit Exceeded Notifications** – A "filter hit" is when a user is blocked by Chaperon when attempting to access a site contained in the Chaperon filter. The Chaperon Activity Monitor accumulates filter-hit statistics on every user using the ISA Server and uses these statistics to calculate a dynamic filter-hit limit. If a user exceeds this calculated limit, a notification is generated for that user with details on the activity triggering the event. These notifications are sent to every specified recipient by default.
- **Suspect URL Access Notifications** – The Chaperon Activity Monitor compares each URL not contained in the Chaperon filter against a list of words, combinations of words, and patterns, which typically indicate a client is attempting to circumvent the filter. When a URL match occurs, a notification is generated for the user with information on what triggered the event. These notifications are sent to every specified recipient by default.

3.a Configuring SMTP Server Settings

1. In the Chaperon Control Panel, navigate to the connections tab.
2. In the "SMTP Server" section, enter the name or IP address of the SMTP server that you want Chaperon to use in order to send its notifications.
3. In the "Email From Address" section, enter an email address (doesn't have to exist) that you want the Chaperon notification emails to appear to originate from when they are received. The domain used in this address should coincide with the domain used on the mail server. For Instance, if email addresses from that server use username@yourdomain.com, then "yourdomain.com" is the domain that should be used in Chaperon's from address. In this example, Chaperon@yourdomain.com would be an acceptable address.
 - **Note:** If your mail server is on the same network as the ISA Server, then your mail server probably doesn't require authentication from clients on that network. If this is the case, go to step 8, otherwise continue to step 4. If authentication information is used when it is not needed, the mail server may discard the messages from Chaperon and Chaperon will show an SMTP error in its service log.

4. Click the button with the toolbox image located next to “SMTP Server” section.
5. Check the “Server Requires Authentication” box.
6. Enter a valid Username and Password for an account allowed to send mail using the SMTP server.
7. Click OK.
8. Click Save on the Connections tab.

3.b Configuring Notification Recipients

3.i Editing the default notification recipient

Chaperon comes pre-configured with a default notification recipient entry. This entry is for the recipient or recipients that will receive all chaperon notifications regarding Chaperon itself, and all notifications regarding user activity. This is the only entry that notifies for Chaperon service events such as filter renewal notifications, service start/stop, any Chaperon errors, and software update availability. The following instructions outline the editing of this entry.

1. In the Chaperon Control Panel, navigate to the Notifications tab.
2. Click the existing entry for “<all usernames> <all ip addresses> <not specified>”.
3. Click the Edit button.
4. The Username and IP Address sections will contain an * and cannot be specified within this default entry.
5. In the Email Address section, enter the email address of the recipient that the notifications should be sent to.
6. Click Add. Repeat steps 5 and 6 for additional recipients for this list.
7. Click OK.
8. Click Save on the Notifications tab.

3.ii Adding New Notification Recipients

The following instructions outline creating new notification entries. These entries will notify for user-activity only and not Chaperon service events.

1. In the Chaperon Control Panel, navigate to the Notifications tab.
2. Click the New button.
3. In the Username section, enter the client username of the user the recipients in this list will receive notifications for. For all users, add only an *. Using * is recommended if specific IP's are specified in step 4.
4. In the IP address section, add the IP address for the clients the recipients in this list will receive notifications for. For all IP's, add an * in the first box only. Using * is recommended if specific usernames were added in step 3.
 - **Note:** Wildcards can be used for IP entries to specify certain subnets. For instance, if someone wanted to receive notifications for all users in the 10.0.0.0 network, an IP could be added as “10.0.0.*” (Without quotes).
5. In the Email Address section, enter the email address of the recipient that the notifications should be sent to.

6. Click Add. Repeat steps 5 and 6 for additional recipients for this list.
7. Click OK.
8. Click Save on the Notifications tab.

3.iii Setting Notification Recipients Based on Active Directory User Managers

Within Active Directory Users and Computers, each user can have a “Manager” specified which is configured on the Organization tab of the user properties. This Manager is essentially another Active Directory user that can be specified. Chaperon can be set to notify the individual specified as the Manager for that particular user’s activity if the user has a Manager specified, and if that Manager has an email address configured in their Active Directory user properties. The following lists the steps needed to configure Chaperon for the ability.

1. In the Chaperon Control Panel, navigate to the notifications tab.
2. Click the Advanced button.
3. On the Monitoring tab, check the box stating “Send a copy of Notifications to User’s Manager listed in Active Directory”.
4. Click OK.
5. Click Save on the Notifications tab.

3.c Setting Which Chaperon Categories to Receive Notifications For

For each Chaperon category, Chaperon can be configured whether or not it will send notifications for that particular category. Some categories such as Adult Material should generate notifications while categories such as Ad Banners usually will not. Chaperon comes preset with certain categories set to notify with others not. The steps below outline the steps needed to configure each category for its notification status.

1. In the Chaperon Control Panel, navigate to the “Filter Categories” tab.
2. Each Chaperon Category will be listed and have a Yes or a No to indicate whether or not notifications will be sent for this category. To switch the status of a category, simply click it’s current status to change it. All “Yes” entries will flow above all “No” entries.
3. Click Save on the “Filter Categories” tab.

Note: Chaperon notifies for categories in the order they fall in this list. For instance, if a website fell into two separate blocked categories, a notification would be generated for the category that was closest to the top. The “Move Up” and “Move Down” buttons are provided so that categories can be placed into a specific order if needed. Categories that are more serious should be placed higher in the list.

4. Setting Chaperon Category Redirect Pages

Each Chaperon category has a specific redirect page it uses for each category. These pages are what the user is redirected to when they try to access a site contained in a filtered Chaperon category. By default, each category is redirected to a CornerPost block page that specifies the Category the particular site is contained in. Each category's redirect page can be separately specified to any URL. To Change a redirect page, complete the following steps for each category you wish to change.

1. In the Chaperon Control Panel, navigate to the "Filter Categories" tab.
2. Click the category you wish to edit.
3. Click the Edit button.
4. In the "Redirect To" section, enter the full URL (including http://) to redirect users to who are blocked from a site in this category.
5. Click Save on the "Edit Filter Category" window.
6. Click Save again on the "Filter Categories" tab.

The new redirect page will take effect after the next filter update or filter reconcile.

5. Configuring the Filter Update Schedule

When Chaperon performs its filter update, it contacts the CornerPost filter servers to download any new additions to the filter list and adds them to the filtering policy. Chaperon also checks for any policy changes that were made locally that haven't been applied yet, and applies them if necessary. The filter update occurs every two hours by default but can be set for any time frame on the hour. The following outlines the steps necessary for editing the update schedule.

1. In the Chaperon Control Panel, navigate to the Enterprise Settings tab.
2. Press the button with the calendar image that is next to the Rules Engine Server setting.
3. Using the mouse, drag over the appropriate day and time sections using the Allow and Deny buttons to set the times. The update will be allowed to start in time frames colored green, while time frames colored white will not allow updates to start.
4. Once your update schedule is set properly, Click OK.
5. Click Save on the Enterprise Settings Tab.

6. Entering Your Registration Key

1. In the Chaperon Control Panel, navigate to the Enterprise Settings tab.
2. Click the Register button.
3. The Registration properties window will open. Click Change.
4. Enter the organization name and serial number exactly as was supplied.
 - **Note:** The organization name and serial number as a pair form your registration. The serial number will not contain a letter o, but only zeros. If either the organization name or serial numbers are incorrectly entered, the changes cannot be saved.

5. Once the pair have been entered correctly, a message should state “Registered (xx Edition), thank-you” and the Save button will be available. Click Save to commit the changes.
6. Your expiration date is retrieved from the filter update server so your expiration date may still appear wrong until a filter update is performed. Do so by navigating to the Dashboard tab and click the “Update Filter” link. Chaperon will update using the new registration key and will change your expiration date to correctly reflect your account.

7. Things to Remember

- Certain Chaperon tabs or windows may take a few moments to open the very first time they are opened, please be patient.
- Most changes within Chaperon require a save to be performed. Save buttons are grayed out when no saves are pending, but available when something hasn't been saved yet. Another way to check if saves are pending is to click the Settings menu button in the Chaperon Control Panel. Any tab names with (*) on the end have pending changes that need to be saved.
- A “Reload Policies” should not be used during normal operation. It is available only to reload the Chaperon objects into ISA if a situation arises that requires it.
- Any Changes made to a Chaperon policy or user-defined filter will not take place until the next filter update. The filter update will happen automatically based on your filter update schedule, but to update the filter immediately, the “Update Filter” link can be clicked on the dashboard tab.
- Changes cannot be made to Chaperon and should not be made to ISA while Chaperon is performing a filter update or filter reconcile. The “Rules Engine” section of the Dashboard tab in the Chaperon Control Panel will state “Idle” if neither of these processes are occurring. If that is not the case, please wait until Chaperon has completed the process before making any changes.
- For any topics or sections of Chaperon not covered in this manual, refer to the help section of Chaperon located under “Help > Chaperon Help” in the Chaperon Control Panel. Additionally, information can be found by clicking the small blue question buttons located on each section of Chaperon.

Microsoft, Active Directory, ISA Server, Internet Security and Acceleration Server, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other Countries.