
BEST PRACTICE: “AGING OUT” HOSTS AND USERS

DATE: 12.29.2011

REVISED: 08.17.2017

Overview

By default, registered host and user records remain in the Network Sentry database indefinitely, and unregistered (rogue) hosts are removed after 30 days or 14 days if inactive.

The best practice is to specify an aging property so at some point in the future, the host or user will “age out” and be removed from the database. This prevents records from being unnecessarily retained in the database when not being used. This feature is particularly useful for managing users and hosts that have been inactive for a lengthy period of time, and for “guests” who need temporary access to network resources.

The following pages provide explanations and recommendations for various methods of establishing aging properties (setting expiration times).

Methods for Setting Expiration Dates

Directory: If the **Time To Live** option is enabled in the **Directory Attribute Mappings** window, the value stored in the Directory is used to calculate the dates for Expiration Date and Inactivity Date.

Global Aging (illustration on page 4): If the **Time To Live** option in the Directory is not being used, then the age times on the **Aging** view are used to populate Expiration Date and Inactivity Date for hosts as they are added to the database and Expiration Date for users.

Note: Changes made to these settings will be applied to existing hosts or users that currently have no value set. In addition, these aging settings will also be used for new hosts or users that are created. Note that the age settings within Network Sentry Properties will apply only when the settings are *not* provided by the directory or group membership.

Group Aging (illustration on page 5): A host group can be created and Group Aging can be used to populate the Expiration Date and/or the Inactivity Date fields for hosts in that group. If a host is moved to a group which has these aging fields populated, the host will take on the group aging values. If the group aging values are edited while there are hosts in the group, the aging values of the hosts who belong to the group will also change.

Note: These changes will not apply to any host whose corresponding Host Aging window has **No Expiration** selected. Expiration settings can be viewed for a particular host by navigating to **Hosts > Host View > Host Properties**.

Associated Hosts Should be Deleted When Aging Users (illustration on page 3): Under the **Users** section of the **Aging** view, there is a checkbox entitled **Delete hosts registered to user upon expiration**. When checked, the host utilized by a user to access the network will automatically be removed when that user is aged out of the system. If left unchecked, the host converts to a registered device in the database.

Individual Overrides

Host Aging: Expiration Date and/or the Inactivity Date values can be entered or overridden for individual hosts. This is done by clicking the **Set** button on the **Host Properties** window or using the **Set Host Expiration Date** option on the **Host View**.

Note: If **No Expiration** is selected, the host is never deleted from the database even if global or group aging options are added or modified. Expiration settings can be viewed for a particular host by navigating to **Hosts > Host View > Host Properties**.

User Aging: Expiration Date and/or the Inactivity Date values can be entered or overridden for individual users. This is done by clicking the **Set** button on the **User Properties** window or using the **Set User Expiration Date** option on the **User View**.

Note: If **No Expiration** is selected, the user is never deleted from the database even if global or group aging options are added or modified. Expiration settings can be viewed for a particular host by navigating to **Users > User View > User Properties**.

Admin User Aging: Administrator users default to No Expiration. When the Expiration Date is set to No Expiration, changes to other global aging options do not affect Administrators.

Guest Aging: A Guest user's expiration date is set based on the Account Duration entered in the Guest Template used to create the Guest.

Configuring Aging in Network Sentry Properties

1. Navigate to **System > Settings > Aging**.
2. Modify the settings (recommended to check **Delete hosts registered to user upon expiration**).
3. Click **Save Settings**.

For further details on each option in this view, see “**Network Sentry - Aging**” topic in online Help.

The screenshot shows the Network Sentry Settings interface. The top navigation bar includes "Settings", "NETWORK SENTRY / RTR", and "Log Out". Below the navigation bar, there are tabs for "Bookmarks", "Users", "Hosts", "Network Devices", "Logs", "Policy", "System", and "Help". The left sidebar shows a "Folder View" with various settings categories, and "Aging - Users/Hosts" is selected. The main content area is titled "Aging - Users/Hosts" and is divided into three sections: "Unregistered Hosts", "Registered Hosts", and "Users".

Unregistered Hosts

- Days Valid:
- Days Inactive:
- Clear Aging values for all unregistered hosts (rogues).

Registered Hosts

- Days Valid:
- Days Inactive:
- Clear Aging values for all registered and guest hosts.

Users

- Days Valid:
- Days Inactive:
- Delete hosts registered to user upon expiration
- Clear Aging values for all users.

Note:
Clear operations will not clear hosts or users that are set to never expire.
Changes made to these settings will be applied to existing hosts or users that currently have no value set.
These aging settings will also be used for new hosts or users that are created, when the settings are not provided by the directory or group membership.

Configuring Group Aging

1. Select **System > Groups**.
2. Use the **Filter** panel to locate the appropriate group.
3. Select the group of type **Hosts**.
4. Right-click on the group and select **Set Aging**.
5. Enter a number for **Days Valid** or **Days Inactive**. The number in Days Valid is used to calculate the Expiration Date for each host in the group. The number in Days Inactive is used to calculate the Inactivity Date for each host (to set the host to never expire, set each value to a very large number, example 9999).
6. Click **OK**.

The screenshot displays the Fortinet Network Sentry / RTR Groups management interface. The main window shows a list of groups with the following columns: Name, Type, Owner, Members, Days Valid, Days Inactive, and Description. A 'Set Aging' dialog box is open over the 'Domain Computers' group, allowing the user to enter values for 'Days Valid' and 'Days Inactive'. The dialog has 'OK' and 'Cancel' buttons. The background interface includes a navigation bar with 'System' selected, a filter panel, and a table of groups.

Name	Type	Owner	Members	Days Valid	Days Inactive	Description
Authentication-Training-Ports	Port	User	3			Authentication managed ports of domain Train
Authorized Access Points	Port	System	161			Ports that have authorized access points conn would be dumb hubs or wireless units.
Authorized DHCP Servers	Device	System	0			Authorized DHCP servers.
BIGGROUP	Host	User	45			
BYOD	Host					
BYOD port group	Port					Enter Group Description.
Backup Operators	Host					
CMAAdmin	Host				000	
Cert Publishers	Host					
Classrooms	Device					
Dave Group	Device					Test
Denied RODC Password Replication Group	Host					
Device Interface Status	Device	System	67			Devices that participate in the updating of devi
DistGroup	Host	User	0			
Domain Admins	Host	User	8			
Domain Collectors	Host	User	0			
Domain Computers	Host	User	0			
Domain Controllers	Host	User	0			
Domain Guests	Host	User	0			
Domain Users	Host	User	0			
Dorm Room	Device	User	2			
Drew-Test	Host	User	0			
Email-gma	Administrator	User	1			
Employee Ports	Port	User	0			Enter Group Description.
Eng-test-port-group	Port	User	1			Engineering test port group
Enterprise Admins	Host	User	6			

Configuring Individual Overrides

Host Aging:

For further details on each option in this view, see “**Set Host Expiration Date**” topic in online Help.

1. Select **Hosts > Host View**.
2. Use the Quick Search or Custom Filter to locate the appropriate Host(s).
3. Select the hosts to be modified.
4. Right-click or click Options and select **Set Host Expiration**.
5. Click the **Set Host Expiration** checkbox. This allows the options below to be edited.
6. Select the desired expiration type and enter expiration criteria (to set the host to never expire, select **No Expiration**).
7. To set an expiration time for hosts who have not been online, select **Set Host Inactivity** checkbox and select the desired expiration type.
8. Click **OK** to set the expiration dates.

The screenshot displays the 'Host View' interface in Network Sentry / RTR. A 'Set Host Expiration' dialog box is open, allowing configuration of host expiration settings. The dialog includes the following options:

- Set Host Expiration
 - Specify Date: [Date Picker]
 - Days Valid from Now: [Input Field]
 - Days Valid from Creation: [Input Field]
 - No Expiration
 - Default Expiration
- Set Host Inactivity Limit
 - Days Inactive: [Input Field]
 - No Inactivity Limit
 - Default Inactivity Limit

The background table shows a list of hosts with the following columns: Status, Host Name, Host Role, Registered To, Logged On User, and Host Created. The table is currently displaying 10 hosts, with the first one being SEP002290B9B88D.

User Aging:

For further details on each option in this view, see “**Set User Expiration Date**” topic in online Help.

1. Select **Users > User View**.
2. Use the Quick Search or Custom Filter to locate the appropriate User(s).
3. Select the users to be modified.
4. Right-click or click Options and select **Set Expiration**.
5. Use the field definitions table below to enter expiration criteria.
6. Click **OK** to set the expiration dates.

The screenshot shows the 'User View' interface in the Fortinet management console. A 'Set User Expiration' dialog box is open, allowing configuration of user expiration and inactivity settings. The background shows a table of users with columns for Status, First Name, Last Name, User ID, Email, Phone, and Mobile Number. The dialog box includes the following options:

- Set User Expiration
 - Specify Date: [Date Picker]
 - Days Valid from Now: [Input Field]
 - Days Valid from Creation: [Input Field]
 - No Expiration
 - Default Expiration
- Set User Inactivity Limit
 - Days Inactive: [Input Field]
 - No Inactivity Limit
 - Default Inactivity Limit
- Delete Registered Hosts when User Expires: Yes [Dropdown]

Buttons for 'OK' and 'Cancel' are visible at the bottom of the dialog box. The background interface includes navigation tabs (Adapter View, Host View, User View, Application View) and a top navigation bar with 'Users' selected.

Admin User Aging: To change the Admin aging from the default of “No Expiration,” follow the same steps as outlined for **User Aging**.

Guest Aging: A Guest user's expiration date is set based on the **Account Duration** entered in the Guest Template used to create the Guest. Templates can be viewed, modified or created by navigating to:

Users > Guest/Contractor Templates

The host registered to the Guest inherits its expiration date from the Global Aging settings. When the Guest user's account expires, both the Guest user's account and the guest's registered host are automatically removed from the database. If the host's expiration date is earlier than the Guest user's expiration date, the host is removed from the database, but the Guest user account remains.

For further details on each option in this view, see “**Guest Manager Implementation**” topic in online Help.

Manually Deleting Users

If a user is manually removed from the Network Sentry Database, it is recommended any associated hosts be removed as well. Otherwise, if there is no associated user, the host converts to a registered device in the database.

To remove both the user and the associated host(s):

1. Navigate to **Users > User View**
2. Highlight the user to be deleted.
3. Click **Delete** at the bottom of the screen, or right click on the user and select **Delete User(s)**.
4. When prompted to delete all registered hosts, check the box.

The screenshot shows the 'User View' interface in Network Sentry. A 'Delete User' dialog box is open, asking for confirmation to delete a user. The dialog includes a checkbox for 'Delete Hosts Registered to User', which is checked. Below the checkbox, a warning message states: 'If hosts are not deleted, they will become registered devices. If one of those devices connects in the future, the user will not need to register and the device will not be associated with the user.' The background shows a table of users with the following data:

Status	First Name	Last Name	User ID	Email	Phone	Mobile Number	Mobile
▶		Training	training				
▶	Kiosk	Concord	ConFrontDesk				
▶	Front	Desk	frontdesk				
▶	Christine	Schneider	CSchneider@mfa-cpa.com	CSchneider@mfa-cpa.com			
▶	Josh	Doss	JRose@mfa-	JDoss@mfa-cpa.com			
▶							
▶							
▶							
▶							
▶							
▶	Bob	DeGregorio	00:22:90:5A:5F:45		2082		
▶	Matthew	Fish	00:22:90:59:E7:6E		1387		
▶	Ajay	Aggarwal	00:22:90:05:BD:C7		2004		
▶	Mike	Gadoury	00:22:55:D4:BE:02		1305		
▶	Mau - Westford	Conf	00:04:F2:E1:6C:E4		2090		
▶	Bahamas	Conf	00:04:F2:E1:6F:A4		2091		
▶	Jamaica	Conf	00:04:F2:E1:72:76		1323		