

# NAV Alert Manual

Andreas Åkre Solberg  
Andreas.Solberg@uninett.no

5th August 2003

# Preface

This manual for NAV Alert is separated into three. First, a short introduction for simple usage. Then more advanced settings for the more experienced user. And last information about NAV Alert administration.

The manual require fundamental knowledge to Internet, how to use a Internet browser, and familiarity with the NAV system.



Figure 1: Screenshot overview of the NAV Alert interface.

Since the webdesign of the webportal was not freezed before this manual was written, the screenshots throughout the manual will depart some visually from your NAV installation.

# Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Terminology . . . . .	4
<b>2</b>	<b>Simple usage</b>	<b>6</b>
2.1	Login . . . . .	6
2.2	Navigation . . . . .	7
2.3	Languages . . . . .	7
2.4	My addresses . . . . .	8
2.5	My profiles . . . . .	9
2.5.1	Alerting service . . . . .	10
2.6	Sorting . . . . .	11
2.7	Icons . . . . .	11
2.7.1	Overview icons . . . . .	11
2.7.2	Standard icons . . . . .	12
2.7.3	Address icons . . . . .	13
2.7.4	Equipment group icons . . . . .	13
2.7.5	Log icons . . . . .	14
2.8	My usergroups and permissions . . . . .	14
2.9	Change password . . . . .	15
2.10	Scenario: My first profile . . . . .	15
<b>3</b>	<b>Advanced usage</b>	<b>17</b>
3.1	Advanced profiles . . . . .	17
3.1.1	Timetables . . . . .	17
3.1.2	Alert queueing . . . . .	19
3.1.3	Scenario: An advanced profile . . . . .	19
3.2	My own equipment groups . . . . .	21
3.2.1	Filtermatch . . . . .	22
3.2.2	Equipment filters . . . . .	22
3.2.3	Equipment groups . . . . .	23
3.3	Using WAP . . . . .	24

---

<b>4</b>	<b>Administration</b>	<b>26</b>
4.1	Users . . . . .	26
4.2	Usergroups . . . . .	26
4.3	Match fields . . . . .	26
4.4	Shared equipment groups and filters . . . . .	28
4.5	Logging . . . . .	29

# Chapter 1

## Introduction

Mainly NAV Alert is a webinterface for administration of NAV-users and a portal where users can login and set up the NAV alert service. Users can save more alert setup through the concept of profiles. An alert service setup is analogous to a profile. Here are some examples of what profiles could be like:

- *Standard*
- *Vacation*, no alerts to mobile. Only most significant to weekly e-mail digest.
- *On watch*, detailed alerts to both e-mail, and IRC or Jabber.
- *Out of town*, alerts only on the most significant.
- *Night duty*, significant alerts to SMS/mobile.

Zero or one profile can be active at a time. No active profile will result in no alerts.

For each profile there is a timetable. For each time period on the time table, rules can be applied for which events will be alerted, which address the alerts should go to and if the alert should be immediately sent or enqueued.

NAV Alert has a simple and flexible system for how to decide which equipment you want to *watch*.

### 1.1 Terminology

Here follows a short summary of the terminology used throughout this manual and in the NAV Alert interface. Concepts are not explained here, but this section can be used as reference for connecting together the concepts.

**Users** are members of **user groups**. Users have a **login name** and a **password**. A user can be member of arbitrary many user groups. Through the user group the user gets **permissions** to a set of **equipment groups**, to which he can setup **alert service subscriptions**.

A user can define arbitrary many **profiles**, but mostly one active at a time. A profile is analogous to a **timetable** with **time periods**, each related to a set of rules deciding which equipment group to alert, which **address** to send the **alerts**, and whether to send immediately or enqueue.

**Equipment groups** consist of a ordered list of equipment filters. A filter can be **included** or **excluded**, and you can optionally include or exclude the inverse of filters. An equipment filter consists of a set of **filtermatches**. For an equipment group to match an event, *all* of the corresponding filtermatches must evaluate to true. A matchfield is a boolean expression consisting of a **match field**, an **operator** and a **value**.

# Chapter 2

## Simple usage

For normal users, there is no need to touch the most advanced features of NAV Alert. This chapter describes the fundamental needed for all NAV Alert users. The more advanced features will be described in chapter 3.

### 2.1 Login

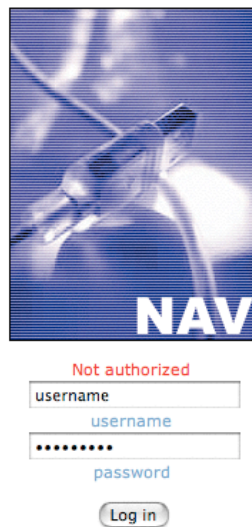


Figure 2.1: Login page to NAV Alert.

To start using NAV Alert you need the following:

- **The webaddress** where NAV Alert is located.
- **An username**, probably the same used for login on computers in your organization.

- A **password**, ask your system administrator if you do not have one.

Figure 2.1 shows an example of a login window. Enter your username in the upper inputfield and your password in the lower inputfield. Then hit the login button.

You can also login on the front page of NAV, and you will **not** have to reenter your password when you visit the NAV Alert interface. When you leave the computer or is finished, press the logout button.

## 2.2 Navigation

Navigation between subsection of NAV Alert is done by using the navigation menu found on the left side of the webinterface. This might look like figure 2.2.

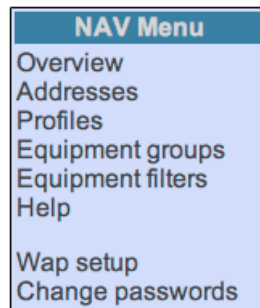


Figure 2.2: The NAV Menu.

What menu items shows up on the NAV menu depends on whether your account is normal user or administrator. The menu on figure 2.2 is for a normal user.

## 2.3 Languages

NAV Alert is multilingual. Current version of NAV Alert contains *english* and *norwegian*. Switching between languages is done by using the language bar is found in the left column of NAV Alert, and looks like figure 2.3.



Figure 2.3: The language bar.

Your current language is highlighted, and the other are dimmed. When you are logged in and choose a language, the choice is saved to your preferences, so it will be the default when you log in next time.



## 2.4 My addresses

Most probably your account already contains your e-mail address. You might want to change your e-mail address, add more e-mail addresses, or add your mobile telephone number for SMS alerts. This is all done under the **addresses** subsection found on the menu.

Class	Address	Options..
E-mail	demouser@ntnu.no	
E-mail	special-alert-address@ntnu.no	
SMS	99887766	

[ update ] Number of addresses: 3

### Add new address

Addressclass: E-mail

Address:

Could be i.e.:  
mail: bruker@uninett.no  
sms: 99372612  
irc: nick@irc.homelien.no  
icq: 123456789

Add new address

Figure 2.4: The addresses section

Figure 2.4 shows the address section, where you can create, edit and delete addresses. There is no limit of how many addresses your are allowed to create, but remember you have to setup at least one to setup any alerts. When you delete an address that are in use in some profile, all alerts setup to that special address is recursively deleted. Therefore you often want to edit an address rather than delete it and add a new one.

Remember that not all users are allowed to setup alerts to mobile phones. The overview section will tell you whether you are allowed or not.

The current version of NAV Alert allow only SMS and E-mail. Further version might include IRC, ICQ, Jabber and more. Feel free to contact the NAV-developers about your preferred way to receive alarms.

The icons for editing and deleting addresses is explained in section 2.7.

## 2.5 My profiles

As mention in the Introduction, a user can setup different alert service rules, meeting different demands, i.e. *Standard*, *Vacation*, *On watch*, *Out of town* and *Night duty*. Each profile contains a timetable with alert service rules. To edit your profiles, choose Profiles from the menu. The section looks like figure 2.5.

The screenshot shows a web interface titled "Mine profiler". It contains a section "Here you can setup and add profiles." with a link "Add new profile". Below this is a table titled "Your profiles" with columns: Active (checkbox), Name, #periods, and Options.. The table lists five profiles: Standard (active), Night duty, On watch, Out of town, and Vacation. Each profile has three icons in the Options.. column: a document with a pencil, a document, and a trash can. Below the table is a status bar: "[ Deaktiver aktiv profil | oppdater ] Number of profiles: 5". At the bottom is a form titled "Add new profile" with fields for Name, Weekly alerts (Monday 09 : 00), and Daily alerts (07 : 30), and an "Add new profile" button.

Active	Name	#periods	Options..
<input checked="" type="checkbox"/>	Standard	1	
<input type="checkbox"/>	Night duty	1	
<input type="checkbox"/>	On watch	1	
<input type="checkbox"/>	Out of town	1	
<input type="checkbox"/>	Vacation	1	

[ Deaktiver aktiv profil | oppdater ] Number of profiles: 5

**Add new profile**

Name:

Weekly alerts:   :

Daily alerts:  :

Figure 2.5: My profiles

To create a new profile enter the name and press "add new profile". Don't bother with the option named weekly and daily alerts. This are related to queueing and will be explained in chapter 3.

The icons under options means "open and edit", "edit in place (rename)" and "delete". The list of profiles contains the number of time periods the profile consists of. The icons are more detailed explained in section 2.7.

You choose which profile to be active by clicking on the icon under the "active"-column.

### 2.5.1 Alerting service

To setup a profile, open the standard profile by clicking on the open icon. Then you see a timetable like the one in figure 2.6.



Figure 2.6: Edit the standard profile

We will not bother with the timetable yet. The profile contains a single time period. This time period starts 8 AM in the morning and ends 8 AM in the morning every day, both weekdays and weekends. Open this time period by clicking the open icon. Then you see a window for setting up alert service rules for that specific time period between the two timetables. See figure 2.7.

Choose equipment to be monitored and alerted to which addresses

Owner	Equipment		#periods	#filters
My computer	E-post	Yes	demouser@ntnu.no	special-alert-address@ntnu.no
	E-post	In queue (daily)		
	SMS	Yes	99887766	
	All servers I have permission to watch			
All servers I have permission to watch	E-post	Yes	demouser@ntnu.no	special-alert-address@ntnu.no
	E-post	In queue (weekly)		
	SMS	No	99887766	
	Save changes			

Figure 2.7: Edit alert service rules for a time period.

Here is all the equipment groups listed. For each equipment group, all your addresses are listed. For each combination of equipment group and address, you choose

wether you want to be alerted (*yes*) or not (*no*). For e-mail addresses you also have the option to enqueue alerts to a daily or weekly digest. When to send out daily and weekly digest is configured to each profile, and is specified when you create an profile.

## 2.6 Sorting

NAV Alert contains a lot of tables. An example is shown in figure 2.8.
















Name▼	#match▼	#groups▼	Options..
All router ports out of Trondheim	2	×	  
All routers	1	×	  
All Webservers	2	×	  
My computer	1	1	  
Webservers at the university	4	1	  

Figure 2.8: Sortable table with equipment groups.

All tables have column headers. This example have *Name*, *#match*, *#groups* and *Options....* The headers that can be sorted on have an down-arrow after the text, and the text have a light blue typeface. The column that is currently sort-key have an yellow arrow instead.

Chosen sort-keys will be remembered during the whole login session but not between sessions.

## 2.7 Icons

Icons are extensively used in NAV Alert. The intension is to make the interface more user friendly. The degree of user friendliness of course depends on how intuitive the icons are. If you are unsure on some of the icons, this chapter hopefully will be helpful.

The icon explanation is collected in convenient groups.

### 2.7.1 Overview icons

These are the icons used in the overview section.

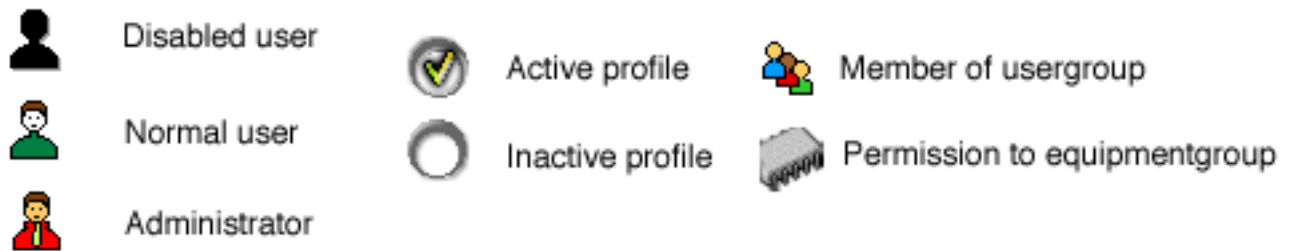


Figure 2.9: Overview icons

The icons; “Normal user” and “Member of usergroup” is somewhere used in a slightly different meaning, where they explain the ownership of an item. Normal user means that the item belongs to the current user, and the usergroup icon means that the current user have access to use the item but it is shared among many users.

## 2.7.2 Standard icons

These are the most used icons, used in a lot of sections.

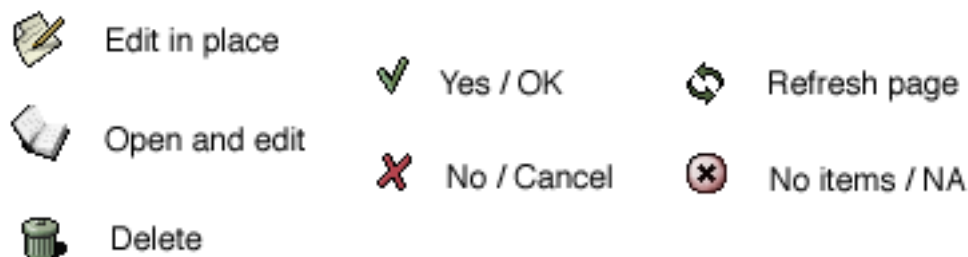


Figure 2.10: Standard icons

The trashcan is pretty selfexplained and is used for deleting an item. What is **very important** to remember is that when you delete an item, you also recursively delete all items that depends on the deleted item. In example when you delete an user you also delete all that users profiles and addresses.

The difference between “Edit in place” and “open and edit” is perhaps not that easy to understand. Edit in place means that you can edit a few of the options related to that item. In example you can edit the name and description. Open and edit, sends you to another section where you can setup that item. In example when you open and edit a profile, you can setup this timetables of this profile. And when you open and edit a time period, you can setup the alert service rules for that specific time period.

The “Yes” and “No”-icons are used to show whether a user has access to SMS or not.

The refresh icon is visible in almost all sections, and clicking on it simply refreshes the page.

The “no items” icon is used somewhere to symbolize zero. Usually 0 relations means that the item is not yet set up properly. Therefore this is emphasized with a special icon.

### 2.7.3 Address icons

These icons are used to visualize different address classes.

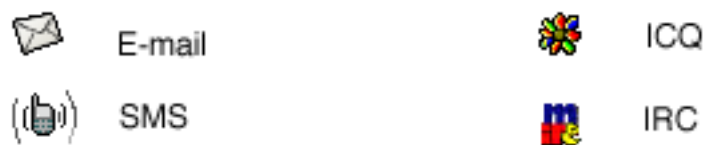


Figure 2.11: Address icons

Your NAV installation probably only contains access to E-mail and SMS, but other address classes will be added in future releases.

### 2.7.4 Equipment group icons

Here are some icons used only for setting up equipment groups. As explained elsewhere setting up equipment groups means constructing a ordered list of inclusion or exclusion of normal or inverse equipment filters.



Figure 2.12: Equipment group icons

The arrows are clickable and allows you to rearrange the order of the equipment filters. When you add an equipment filter you choose between inclusion or exclusion and between normal and inverse.

### 2.7.5 Log icons

The log is only accessible for NAV administrators. More about the log is found in section [4.5](#).

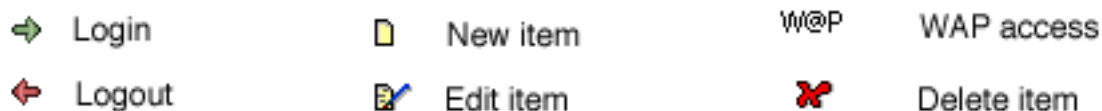


Figure 2.13: Log icons

These are non-clickable illustrative icons related to different type of events logged.

## 2.8 My usergroups and permissions

All NAV users are most probably members of one or more user groups. Through the user group you get access to common equipment groups that you can use in your alert service setup. Permission to what equipment you can watch is also assigned through the user groups.






Usergroups	Permissions
 <b>NAV users</b> Beskrivelse : All users of NAV should be member of this group.	 <b>NTNU-equipment</b> Beskrivelse : All equipment that NTNU owns.
 <b>NTNU employees</b> Description : All employees at NTNU	You have permission to 1 equipment groups.
 <b>NTNU Faculty of Computer Science</b> Description : NTNU Faculty of Computer Science	
 <b>NTNU - Institute for artificial intelligence</b> Description : NTNU - Institute for artificial intelligence	
You are member of 4 usergroups.	

Figure 2.14: User groups and Permissions for the demo user.

The overview section contains a list over all the user groups you are member of and all equipment groups your memberships assign you permission to. Figure [2.14](#) shows an example.

## 2.9 Change password

For security reasons changing password is a good thing. NAV Alert let you do that.<sup>1</sup> Be aware that if you access NAV Alert over an unsecured line<sup>2</sup>, your new password is sent as clear text through the network. This is also the case each time you login.

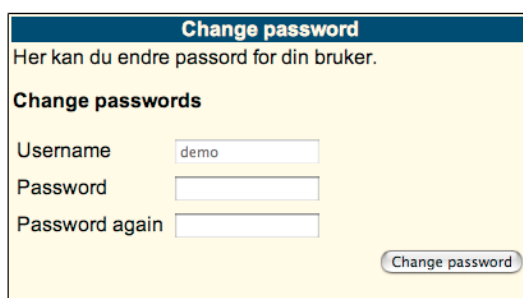
The screenshot shows a web form titled "Change password" in a blue header bar. Below the header, the text "Her kan du endre passord for din bruker." is displayed. The form is titled "Change passwords" and contains three input fields: "Username" with the value "demo", "Password", and "Password again". A "Change password" button is located at the bottom right of the form.

Figure 2.15: The change password section.

Normal users can **only** change their own password. Administrators can change the password of other users.

## 2.10 Scenario: My first profile

Now that you probably have the main idea of what NAV Alert is about, let us create a simple user profile. You want to create a standard profile. The standard profile already exist so you open and edit it. Your system administrator have perhaps helped you to set up your personal computer as a separate equipment group. That is the case for our demo user. In addition we have access to two common equipment group "All servers", "All web-servers at the university" and "NTNU-gw". You have a mobile phone, and access to get SMS alerts, and two work e-mail addresses and a private e-mail address, which will be sorted into different folders in your e-mail client. You want the following alert service setup:

- You want alerts regarding your personal computer to be sent to your private e-mail immediately. No alerts to SMS.
- You want a weekly digest e-mail summary for all servers you have permission to. This should be sent to the special-alert-address@ntnu.no, in which you use for alert-digests. No SMS alert here.

<sup>1</sup>Be aware that NAV supports external user sync, and this may cause that password is not changeable through the NAV Alert user interface.

<sup>2</sup>Check whether your address starts with http or https.



- You want immediate e-mail alert for web-servers at the university to your regular e-mail address.
- When NTNU-gw changes state you want immediate alert on SMS. In addition you want a daily digest to e-mail.

To setup this profile, open and edit the standard profile. And open and edit the single time period. Then enter the alert service rules like visualized in figure 2.16

☒ Monday - Friday  
☒ Saturday and Sunday

**Choose equipment to be monitored and alerted to which addresses**

Owner	Equipment	#periods	#filters
My computer	<div>E-post Yes</div> <div>E-post No</div> <div>E-post No</div> <div>SMS No</div>	1	1
All servers I have permission to watch	<div>E-post No</div> <div>E-post No</div> <div>E-post In queue (weekly)</div> <div>SMS No</div>	1	
Webservers at the university	<div>E-post No</div> <div>E-post Yes</div> <div>E-post No</div> <div>SMS No</div>	1	1
Router: NTNU-gw	<div>E-post No</div> <div>E-post No</div> <div>E-post In queue (daily)</div> <div>SMS Yes</div>	1	

Save changes

Figure 2.16: The alert service rules for my first profile.

Now, set the Standard profile as active.

## Chapter 3

# Advanced usage

This chapter covers more advanced features of NAV Alert, including timetables, alert queueing, using WAP and how to setup your own equipment groups.

### 3.1 Advanced profiles

In chapter 2, setup of very simple profiles was explained. Two features was left out, *timetables* and *alert queueing*. These two in combination is a pretty powerful tool, allowing you to get the alert service the way you want it.

#### 3.1.1 Timetables

Timetables is exactly what it sounds like. Timetables allows you to assign different alert service rules to different time periods in a profile.

A profile can have one or more time periods, and each time period have a starting hour and is either assigned to weekdays (mon-fri), weekends (sat-sun) or both. The userinterface for defining timetables have a separate visualization of 24-hour, from a weekday or weekend respectively. So the 24-hour timetable for i.e. weekdays will show a composition of all time periods for weekdays only and time periods for both weekdays and weekends. In addition to a visualization the userinterface list up all the time periods in a table, see figure 3.1.

The example in figure 3.1 shows a timetable for weekdays with five time periods, starting at 08:00, 12:00, 12:30, 18:00 and 23:00. The duration of a time period is given by the start time of the period, and lasts until the next time period starts.

If only one time period exist, the duration will off course be all 24 hours, and the start time, will be irrelevant.

To create a new time period, you have to click on the timetable on the time you want the time period to start. If you click on the weekday timetable, the new time period will be weekdays only, and similar with the weekends timetable. If you want to create

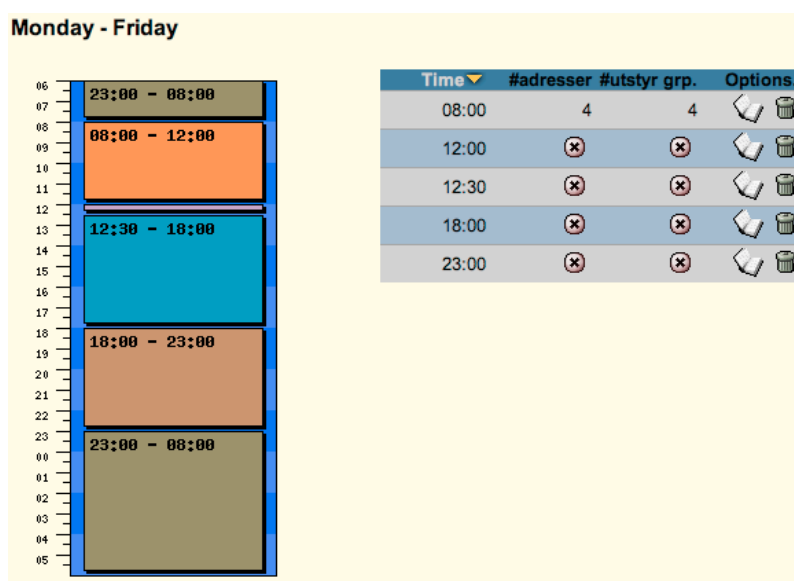


Figure 3.1: An example of a timetable for weekdays.

a time period for both weekdays and weekends, you have to choose one timetable and check both weekdays and weekends checkbox at the alert service setup (see figure 3.2).

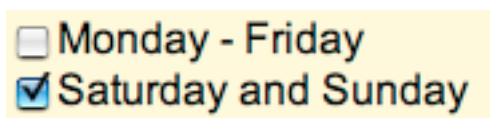


Figure 3.2: Options for a time period.


When you create a new time period, the alert service setup window will appear between the two time tables. Here you can setup alarms for that specific time period. There is also a input field for the starting time for the time period. This is already set when you clicked on the timetable, but you can change the time here, or specify a time with higher resolution, i.e. 08:15.

You can delete a time period by clicking on the trashcan icon.

### Conflicting time periods

If you try to create to time periods with the same start time, and both time periods is assign to either weekdays or weekends, you have a conflict. The web interface will tell you this by showing an alert like the one in figure 3.3, but you have to resolve the conflict yourself. This is done by deleting or alter the time period causing the conflict.

**Conflicts**

 You have created two or more timeperiods which starts at the same time. Delete the superfluous time periods to remove this warning.

Here is a list of the current conflicts:

Dagtype	Tid	Antall kolliderende tidsperioder
hverdag	08:00:00	2

Figure 3.3: Two time periods creating a conflict.

### 3.1.2 Alert queueing

In the alert service setup, there is possible to choose yes and no from the menu. “Yes” means, alert is sent immediately, and “no” means alert is never sent. In addition there is three types of queueing<sup>1</sup>.

Daily queueing means alerts are collected to a queue, and a digest is sent out at the times specified in the profile. The same applies to weekly queues, digests are sent out once in a week at the specified time and day.

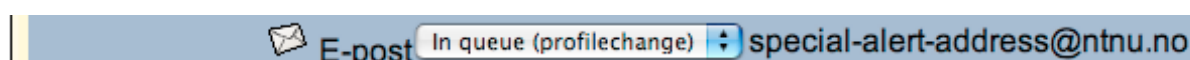


Figure 3.4: Queueing to new time period or profile change.

There is a third kind of queue, shown in figure 3.4. Every time the user profile enters a new time period, or the user switches profile, the queue is checked, and if the alert service rules of the current time period tells the alarm to be sent immediately, the queue is emptied, and a collection of matching alerts from the queue is send immediately. It is very important than when you decide to put alerts in this queue, you have to setup a time period with immediate alert service for the same equipment group, so the queue will not grow against infinity<sup>2</sup>.

### 3.1.3 Scenario: An advanced profile

Let's collect the threads and create a more advanced profile than the scenario in section 2.10. We want a profile matching the following needs:

<sup>1</sup>Queueing for SMS alerts is not implemented in the current version of NAV.

<sup>2</sup>A garbage collector prevents this by deleting “old” alerts. Your user is allowed to enqueue alerts for a given amount of days.

- Weekdays between 08:00 and 16:00 you are at work. From 12:00 to 12:30 you are at lunch. You go to bed about 23:00 at night.
- For NTNU-gw you want alerts to SMS after work, but not when you are asleep. You want alerts for NTNU-gw to e-mail in the working hours. You want alerts to e-mail for NTNU-gw during the working day. E-mail alerts after work hours should be enqueued and sent as a summary the day after when you come to work.
- You want SMS about webserver at the university during the working hours, but not in the lunch break.
- In the weekend you want **no** alerts to SMS.
- All alert services that sends e-mail during the weekdays, should be enqueued during the weekend, and a summary should be sent Monday morning.

We start with creating a brand new profile. This contains a single time period. The first thing we do is changing the time period to only act for weekdays. Then there is no time period at all acting for weekends, so we create a new one for 08:00 at weekends. No there is two different time periods both starting 08:00, but one for weekdays and the other for weekends. Next we create a time period 12:00 for lunch, and a new one 12:30. We create a time period 16:00, acting after work. Last we create a time period 23:00, when we go to sleep. Now the time periods looks something like figure 3.5 and 3.6.

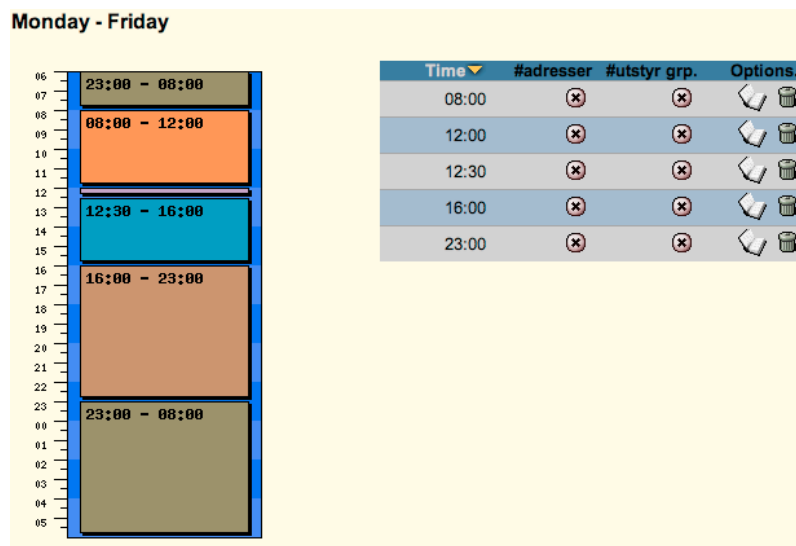


Figure 3.5: Timetable for weekdays.

It is a good tips to never edit an active profile, so before setting up a new profile, be sure another profile is active, or all profiles inactive. The following steps needs to be setup to realize the scenario described above:

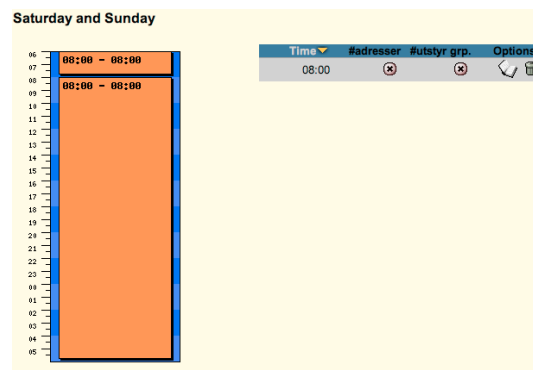


Figure 3.6: Timetable for weekends.

- Open and edit the time period *weekdays 08:00*; edit the alert service to include e-mail alert immediately for NTNU-gw. Add alerts to SMS for “webserver at the university”.
- Open the time period *weekdays 12:30*, and apply the same setup as for the 08:00 time period.
- Open and edit the time period *weekdays 12:00*, which is the lunch break. Add alerts immediately to e-mail for NTNU-gw.
- Open and edit the time period *weekdays 16:00*. Add SMS alert for NTNU-gw. Set alert for NTNU-gw to e-mail to *In queue (profile change)*.
- Open and edit the time period *weekdays 23:00*. Set alert for NTNU-gw to e-mail to *In queue (profile change)*.
- Open and edit the time period *weekends 08:00*, and set it similar to *weekdays 23:00*.

Now the alert service should work as intended.

## 3.2 My own equipment groups

The NAV administrators have probably already configured a collection of predefined equipment groups, that you can use for alert service setup. However, NAV alert allows you to construct your equipment groups. There is no limitation to creation of equipment groups, but for an alert to be sent out, the alert has to match **both** your permissions **and** the equipment groups specified in the alert service setup.

Equipment groups is constructed by including and excluding equipment filters. And an equipment filter is a collection of filtermatches. Therefore it is convenient to go through the creation steps bottom-up.

### 3.2.1 Filtermatch

A filtermatch is an atomic boolean expression. It consists of a match field, an operator and a value. The match field is related to the equipment database, and could be i.e. *location*, *category*, *organization* or *equipment type*. The NAV administrators have the opportunity to add additional match fields.

The set of operators to choose from differ from match field to match field. Examples of operators could be *equal to*, *contains*, *equal or greater than* or *regex*.

There is two possible ways to enter the value. One is simply an input field. The input field should be accompanied by a description of in which format the value should be written, i.e. IP-addresses. The other way to select a value, is a drop-down menu with all possible<sup>3</sup> values, see example in figure 3.7.

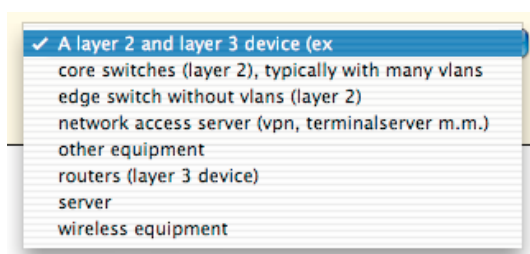


Figure 3.7: Drop-down menu for selecting a category.

### 3.2.2 Equipment filters

An equipment filter is simply a collection of one or more filtermatches. Equipment filters are named and can be attached a description. A single equipment filter could be reused in several equipment groups. When you create a new equipment filter, it is empty, with no filtermatches attached. You can think of an empty equipment filter to match everything<sup>4</sup>, and adding filtermatches adds conditions which limit down the set of alerts. For an equipment filter to match an alert, all filtermatches attached to the equipment filter must evaluate to true. An equipment filter is analog to a boolean expression like (*filtermatch1 and filtermatch2 and filtermatch3 and ...*).

To attach filtermatches to an equipment filter, you should click the open and edit icon for the equipment filter. Figure 3.8 shows an example of the filtermatches of a equipment filter.

<sup>3</sup>The values are dynamically extracted from the equipment database.

<sup>4</sup>Although an empty equipment filter intuitively will match all events, the system is not guaranteed to support empty equipment filters. To create a equipment filter that will match all events, the user is advised to add a single filtermatch like: "*ip address is alike \**".




Filter match			
Field▼	Condition▼	Value▼	Options..
Kategori	is alike	KANT	
Rom	is alike	365	
Leverandr av utstyr	is alike	3com	

Figure 3.8: An equipment filter, a composition of filtermatches.

The example equipment filter in figure 3.8 will match alerts for all *layer 2 devices*, supplied by *3com* located in *room 365*.<sup>5</sup>

### 3.2.3 Equipment groups

Equipment groups are the final goal, and is what will be used directly when setting up alert services. Since each equipment group will be available for alert setup, it is important to keep the number of equipment group so low as possible. Use equipment filters more extensively to create large and more complex equipment groups. For some users creating a single equipment group might be enough. All equipment that you want the same alert service for, should be collected in the same equipment group.

An equipment group is created by including and excluding equipment filters. You **always** start by including a equipment filter, then you might include or exclude an unlimited number of filters, in an ordered list.

Think of an equipment group as a subset of all possible alerts. When you start with an empty equipment group, you have an empty set. Adding a line with inclusion of an equipment filter, will add alerts that match that particular equipment filter to the equipment group. Excluding an equipment filter, will subtract all elements or alerts from the equipment group that match the equipment filter. An equipment group can be composed of an unlimited number of equipment filters. Although the user, is for simplicity reasons, limited to use a particular equipment filter only once in the same equipment group.

In addition the user is allowed to include or exclude the inverse of an equipment filter. Including the inverse of an equipment filter means that all alerts that **is not** matched by the equipment filter will be added to the equipment group. Excluding the inverse of an equipment filter means that all alerts that **is not** matched by the equipment filter is removed from the equipment group.

To setup an equipment group, you should create a new one. Then you have to “open and edit” it to setup the equipment filter list.

<sup>5</sup>Note that the value listed in the table is the database key, and may differ from the more descriptive name found in the drop-down menu.



Explaining the concept of equipment groups with abstract algebra notation is left as an exercise to the reader.

Figure 3.9 shows an example equipment group. This equipment group will match all workstations on the 129.241-subnet (NTNU), except from an evil box and VPN-connected equipment. In addition to this, my home computer is added to the equipment group.

Equipment filters				
Incl	Neg	Equipment filter	Move	Options..
		All personal computers		
		All laptops		
		Equipment on the 129.241 subnet		
		Box: evilbox.ntnu.no (on service)		
		Equipment on the 129.241.200 subnet		
		VPN-connected boxes		
		My nice home computer		

[ update ] Number of filters: 7

Figure 3.9: An example equipment group.

The equipment filter called “My nice home computer” is probably containing a filter-match specifying the MAC-address, of my home computer. Since the equipment filter is added at the bottom of the list, it will be included in the equipment group even if it is connected through VPN. Even if some evil sysadmin attached the `evilbox.ntnu.no` DNS-name to my home computer<sup>6</sup> it will be included in the group. Since the order of equipment filters is so crucial, convenient move-icons are included in the web interface, allowing you to reorder the filters.

The trash can icon, just removes the equipment filter from the equipment group. The equipment filter itself will of course not be deleted.

### 3.3 Using WAP

Some NAV installations might include a simple WAP-portal. This portal allows the user to change active profile from a mobile phone. This could be very useful, if the user gets

<sup>6</sup>Off course no sysadmin is that evil.

a lot of SMS alerts, and i.e. is on vacation, but forgot to change profile before he left his office. The WAP portal allows him to change profile without access to a computer.

If NAV users find the WAP portal very useful, more functions could be implemented in the WAP portal in future versions.

To access the WAP portal, you have to activate WAP for your NAV user. To do that choose WAP setup from the menu. Then choose "Generate wapkey". This will generate a short string specific to your user, you also get an url including this wapkey. When accessing this url from your mobile phone you are automatically logged in with your user, and can choose between your profiles. This url and wapkey should be treated as a password. If you save the url on your mobile phone, everyone with physical access to your mobile phone will be able to change your profile, without password. If you believe your wapkey has been compromised, you want to generate a new wapkey through the web interface, or disable it. Paranoid users might want to change wapkey on a periodically basis. The wapkey is generated at random, and has no relation to your NAV password.

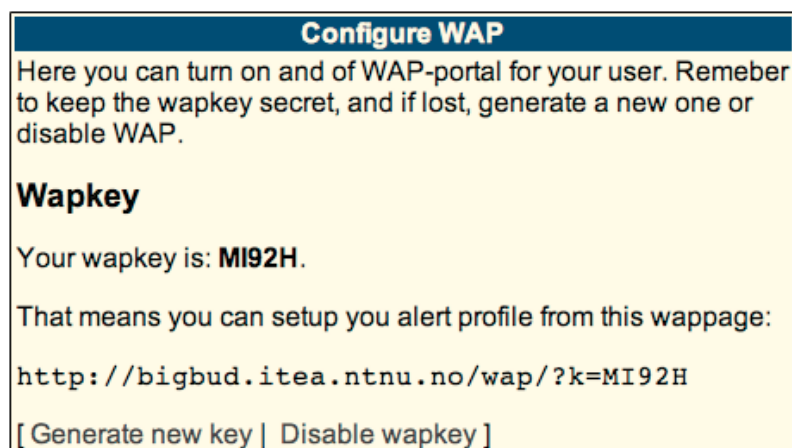


Figure 3.10: WAP setup.

Figure 3.10 shows the web interface for WAP setup.

# Chapter 4

## Administration

NAV administrators have a few extra items on the NAV menu. These includes *Users*, *Usergroups*, *Admin equipment groups*, *Admin equipment filters*, *Match Field* and *Log*.

### 4.1 Users

User administration is moved outside NAV Alert, and will not be covered in this manual yet.

### 4.2 Usergroups

Usergroup administration is moved outside NAV Alert, and will not be covered in this manual yet.

### 4.3 Match fields

Match fields are used when defining filtermatches. To set up match fields, knowledge about the equipment database backend is required. The NAV installation includes a set of predefined match fields. This will be sufficient for most NAV installations.

Figure 4.1 shows the setup section for new match fields. The name is what will be visible when defining filtermatches. The show list option, is where you choose wether the user will be presented for an input field or a drop-down menu for choosing values. The datatype is a helper-option for the alertengine.

Further the options include four relations to the equipment database. These contains dynamically updated drop-down menus contains all table and fields found in the equipment database at the moment. The datatype of the If local NAV hackers have added fields or tables to the equipment database<sup>1</sup> it will show up here. The reference

---

<sup>1</sup>Altering backend database schemes will probably break the rest of the NAV system.

Figure 4.1 shows the 'Creation of a new match field' form. It contains the following fields and options:

- Name:** A text input field.
- Show list:** Two radio buttons, with 'Show list' selected.
- Maks listelengde:** A numeric input field set to 300.
- Datatype:** A dropdown menu set to 'String'.
- Manage (id):** A dropdown menu set to 'camid (int4)'.
- Manage (Name):** A dropdown menu set to 'No reference'.
- Manage (Category):** A dropdown menu set to 'No reference'.
- MAnage (Sort):** A dropdown menu set to 'No reference'.
- Description:** A large text area.
- Verdihjelp:** A large text area.

Figure 4.1: Creation of a new match field.

to Manage (name) and Manage (id) is required. The reference to category and sort is optional.

Figure 4.2 shows the 'Selection of reference to equipment database' dropdown menu. The menu is open, showing a list of fields from two tables: 'cam' and 'cat'. The 'cam' table fields are: camid (int4), end\_time (timestamp), mac (varchar), misscnt (int4), module (varchar), netboxid (int4), port (int4), start\_time (timestamp), and sysname (varchar). The 'cat' table fields are: catid (varchar) and descr (varchar). The 'camid (int4)' field is selected, indicated by a checkmark.

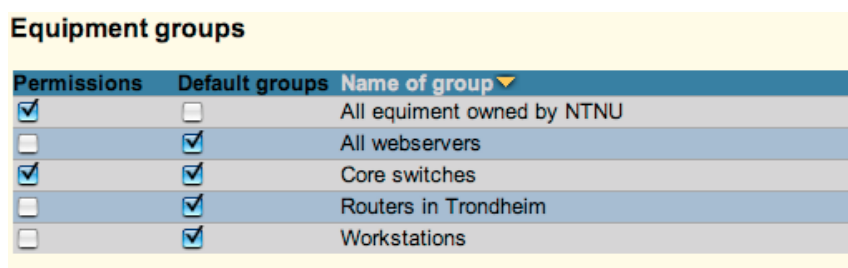
Figure 4.2: Selection of reference to equipment database.

The reference to name, determines what text will be presented to the user in the drop-down menu, when choosing value from list when creating a filtermatch. The id is what will be compared to when an alert is to be checked against a filtermatch. The optional category reference means that all equipment with the same category field will be collected in groups in the drop-down menu. This is very convenient for hierarchal filtermatch values. Sort is a reference to the database field on which the drop-down menu will be sorted. All references to the database **must** be to fields to the same database table.

## 4.4 Shared equipment groups and filters

All users have equipment groups and filters related to their user. In addition there is a set of shared equipment groups and filters. Equipment filters are shared among administrators. All administrators have read and write access to the shared equipment filters. Shared equipment filters can not be used to creating private equipment groups, only to create shared equipment groups.

Shared equipment groups are also shared among all administrators, with both read and write access. Shared equipment groups can also be assign user groups with read access. There is two ways of relating a shared equipment group to an user group. First it could be used to give away **permissions** to users groups. All users member of the user group, get permission to set up alert services for all the alerts available through the shared equipment groups. Second, the shared equipment groups could be used to give **default equipment groups** to user groups. Users member of a user group can use all the default equipment groups to set up alert services.



Permissions	Default groups	Name of group ▼
<input checked="" type="checkbox"/>	<input type="checkbox"/>	All equipment owned by NTNU
<input type="checkbox"/>	<input checked="" type="checkbox"/>	All webserver
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Core switches
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Routers in Trondheim
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Workstations

Figure 4.3: Assigning default equipment groups and permissions to a specific user group.

Although an user might have very limited permissions to receive alerts, the user is free to define as wide equipment groups as wanted. The alert service checks both the equipment group of the profile, and of the permissions, and the alert **must** match both before an alarm is sent out. The setup of permissions and default equipment groups is independent. It is possible to assign a default equipment group to an user, without giving permission to the same equipment group. Likewise you can assign permission to an equipment group without setting the same equipment group as default. This will not prevent the user from being allowed to create an equal equipment group as private.

As a simple example, you can assign an user group permission to access all equipment owned by NTNU, but you don't want that to be a default equipment group. In addition you want to give the same user group a default equipment group called "All webserver". You will indeed not give this equipment group as a permission, because that would allow the user to access alerts for all webserver (also not owned by NTNU). When the user sign up alert services for the default equipment group "All webserver", it will be limited to All webserver owned by NTNU, because of the users limited permissions.

## 4.5 Logging

The NAV Alert performs some limited logging of what is done in the web userinterface.

Logdata			
Event▼	Name▼	Time▼	Description▼
⇒	NAV Administrator	23:50, fre 4 jul 03	Logget inn fra 174.80-202-219.nextgentel.com
⇐	Demouser	23:50, fre 4 jul 03	Logget ut
⇒	Demouser	09:32, fre 4 jul 03	Logget inn fra snow.uninett.no
⇒	Demouser	14:46, tor 3 jul 03	Logget inn fra snow.uninett.no
⇐	NAV Administrator	14:46, tor 3 jul 03	Logget ut
□	NAV Administrator	14:45, tor 3 jul 03	Nytt felles utstyrfilter (NTNU-equipment)
⇒	NAV Administrator	14:44, tor 3 jul 03	Logget inn fra snow.uninett.no
⇐	Demouser	14:44, tor 3 jul 03	Logget ut
⇒	Demouser	14:42, tor 3 jul 03	Logget inn fra snow.uninett.no
⇐	Andreas Åkre Solberg	14:42, tor 3 jul 03	Logget ut
⇒	Andreas Åkre Solberg	14:41, tor 3 jul 03	Logget inn fra snow.uninett.no

Figure 4.4: NAV Alert logging.

The most important is probably log of which users who log into the system, and from where. The system also logs WAP access.