Fusion Web User Manual

Version 1.9.1

Table of Contents

1 Document Introduction

1.1 Document Purpose

The purpose of this document is to give a tutorial on how to use Fusion Web.

1.2 Document Audience

This document is written for Service Provider employees managing the CPE deployment, also referred to as Fusion Operators.

1.3 Document History

Version	Editor	Date	Changes
1.8.0	Jarl André Hübenthal	28-09-10	Initial public release
1.8.1	Jarl André Hübenthal	19-10-10	Update release
1.8.2	Jarl André Hübenthal	12-01-11	Pre-release
1.8.3	Jarl André Hübenthal	07-02-11	Update-release (preliminary)
1.8.4	Jarl André Hübenthal	30-06-11	2011R2
1.9.1	M.Simonsen	16-12-11	2012R1 - updated document with some new chapters, restructured

1.4 Acronyms and Abbreviations

Acronym	Explanation
ACS	Auto Configuration Server.
APS	Automatic Provisioning System.
Fusion	Owera's eXtensible APS with advanced features such as Service Windows, Job Control and Smart Groups.
CPE	Customer Premises Equipment. Used in this document to refer to a single physical device. Same as the term "Device".
Fusion Administrator	Employee of a Hosting Provider managing network infrastructure. Typically the person deploying, configuring and running the Fusion.
Fusion Operator	Employee of a Hosting/Virtual Provider managing the provisioned deployment of CPEs through the Fusion Web Interface.
Parameter	Each individual configuration setting is represented in the Fusion Data Model as a Parameter. A Parameter consists of a name and usually (but not always) a value.
Unit	A dataset in the Fusion database consisting of Parameter values relating to a single CPE. This dataset may extend beyond the Parameter values actually sent to the CPE, as some Parameter values may only be useful or needed by the Fusion itself. Also, the dataset may represent only a subset of all the configurable settings in the CPE. For these reasons, it is important to distinguish the term "Unit" from the terms "CPE" and "Device".
Profile	Dataset stored in the Fusion containing Parameter values shared

	by multiple Units of the same Unit Type. A Unit is always assigned to a single Profile. Multiple Profiles may be created for a Unit Type.
Unit Type	Units that represent CPEs of the same model share a common definition of that CPE model named Unit Type. The Unit Type definition is a list of Parameter names only, as the Unit Type never contains any Parameter values (values are stored in the Unit and/or Profile).
Group	A set of matching criteria used to search for Units. Commonly referred to as Smart Group.
Job	Automates and controls changes to Units within a Group. Partitions the changes over time according to rules to limit network load.
Job Chain	Multiple Jobs being automatically executed in a designated sequence.
Periodic Mode	Provisioning Mode where the Fusion automatically configures all CPEs based on their combined Unit and Profile parameter values.
Inspection Mode	Provisioning Mode where an Fusion Operator manually inspects and configures a single CPE through the Fusion Web Interface.
TR-069	Industry standard provisioning protocol used by the Fusion to read and write configurations from and to the CPEs, in addition to handle upgrades.
IAD	Integrated Access Device (e.g. a router)

1.5 References

Document
[1] Fusion Explained
[2] Fusion Installation
[3] Fusion Monitor Server User Manual

2 Introduction

Fusion Web is the most user friendly interface of Fusion. The goal was to provide users with a simple way of manipulating the contents of Fusion and to provide an easy access to the data that is stored in the database.

Even so, Fusion Web may still be complicated, since many functions are squeezed into a few web pages. This document is a collection of tutorials that covers one or more pages. For in-depth usage of the individual pages, please refer to the help text provided in Fusion Web.

Its necessary to be familiar with the core concepts within Fusion before going about using Fusion Web for production. Therefore it is crucial that the operators can test and tinker with Fusion web in a safe environment. Such a sandbox environment can be provided with a demo account from Ping Communication or by using the hosted solution. In both of these alternatives backups is made nightly so that you are able to rollback any destructive changes made to devices or parameters in the database. Besides demo account and hosted solution, you can also install Fusion in your own test environment.

3 Configuration & Installation

3.1 *xaps-web.properties*

The installation procedure is described in [2], but the configuration must be described here. The first configuration file to look at is *xaps-web.properties*:

```
# --- Session timeout ---
# Defines how long a user can be logged in and inactive
# before he gets logged out automatically.
# allowed input is time in minutes, default is 30
session.timeout = 1440
```

The session.timeout setting defines how long a user can stay logged in as inactive before he is automatically logged out.

```
# --- Monitor Server ---
# where to retrieve monitor status (not including context root and other
# parameters)
monitor.location = http://localhost:8080
```

If the monitor server is installed somewhere, it is made possible to configure the location of where the monitor server is located. If not, turn this functionality off, by setting the enabled-property to 'false'. The monitor server is explained in [3].

```
# --- Database connections ---
# db.maxage and db.maxconn are default values. They can be overriden
# for each defined connection like this: db.1.maxage=70000 or db.1.maxconn=4
db.maxage = 60000
db.maxconn = 10
```

Fusion Web is capable of connecting to various databases, a functionality one might appreciate when multiple databases is present in the set-up. One particular use case might be a set-up with several test servers and several production servers. Each database connection has a maximum age and a maximum number of connections allowed, but default settings will probably do for all the connections.

```
# The format is <user>/<pass>@<url>
# Only MySQL and Oracle database are supported right now.
# If the url doesn't include 'mysql' or 'oracle', the logic will fail.

db.xaps = xaps/xaps@jdbc:mysql://localhost:3306/xapsdb
# db.xaps = xaps/xaps@jdbc:oracle:thin:@//localhost:1521/orcl
```

Subsequently, each database connection is defined by a URL, see figure above. The format is <user>/<password>@<jdbc-url>. Currently Fusion Web support Oracle and MySQL and both JDBC URL formats are shown in the above example. The property is required for Fusion Web to run.

```
# --- Syslog connection ---
# This settings is by default commented out.
# If the Syslog database is on another server than Fusion Web,
# you can specify the url (see format above).

db.syslog = xaps/xaps@jdbc:mysql://localhost:3306/Syslogdb2
```

In some deployment scenarios it might be desirable to keep syslog messages stored in a database separate from the Fusion database. Configure the connection to such a separate syslog database here. For each Fusion database, it is thus possible to configure a separate syslog database. Not required for Fusion Web to run, because the system will fall back to using the xaps database as the syslog database.

3.2 Logging into to Fusion for the first time

When logging in for the first time the Fusion database has no pre-configured users. In this case the system will accept a default username/password combination:

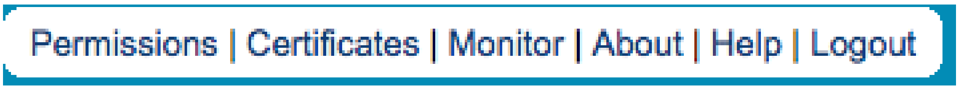
```
Username: admin
Password: xaps
```

Remember to change this password by opening the Permissions menu item (as you can see in the screenshot below) and change the password to a more complex password.

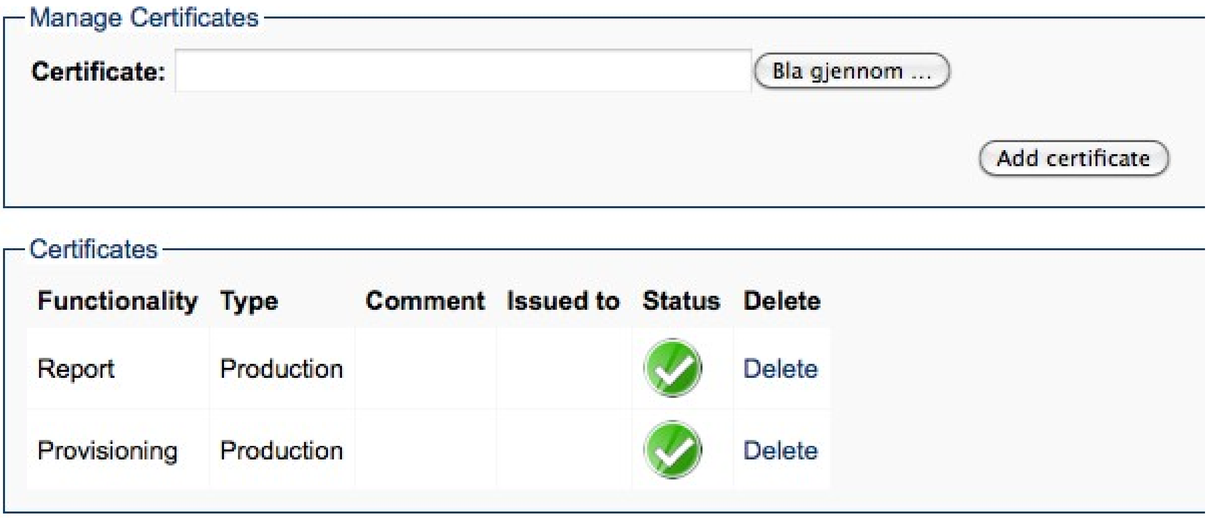
3.3 Installing (if needed) necessary certificates

By default Fusion ships without any pre-installed certificates and Fusion Web will not display any reports and the Fusion TR069 server will not provision any CPEs. To enable provisioning and reporting within Fusion, some certificates must be installed.

First, login as admin. Click on the "Certificates" link in the upper right tools menu.


Permissions | Certificates | Monitor | About | Help | Logout

In the next dialog choose the certificate you wish to install and click the button labeled "Add certificate". As you can see from below, this is what it will look like after the two certificates has been installed. Your company name will be added to the "Issued to" column if the certificates are for production (not trial).

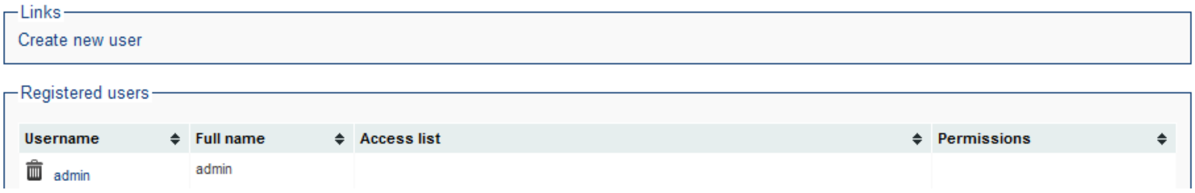


Functionality	Type	Comment	Issued to	Status	Delete
Report	Production			✓	Delete
Provisioning	Production			✓	Delete

4 Basic

4.1 Permissions

Fusion have a permission system to control which pages a user is allowed to see and which Unit Types and Profiles a user can access. Click on the "Permissions" link in the top menu.



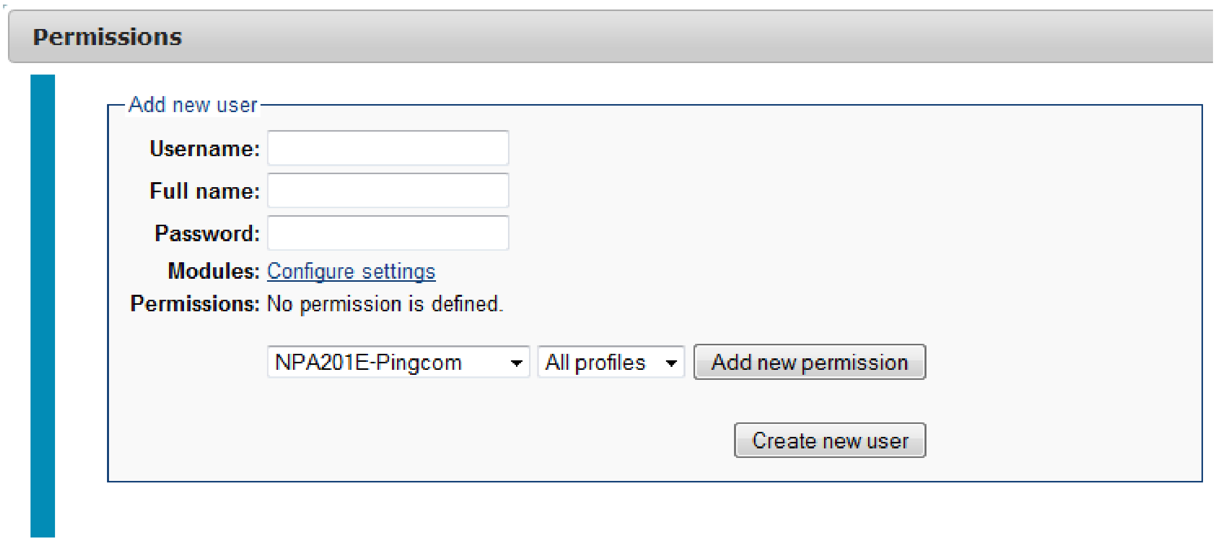
Links

Create new user

Registered users

Username	Full name	Access list	Permissions
admin	admin		

Create a user by clicking on "Create new user":



Permissions

Add new user

Username:

Full name:

Password:

Modules: Configure settings

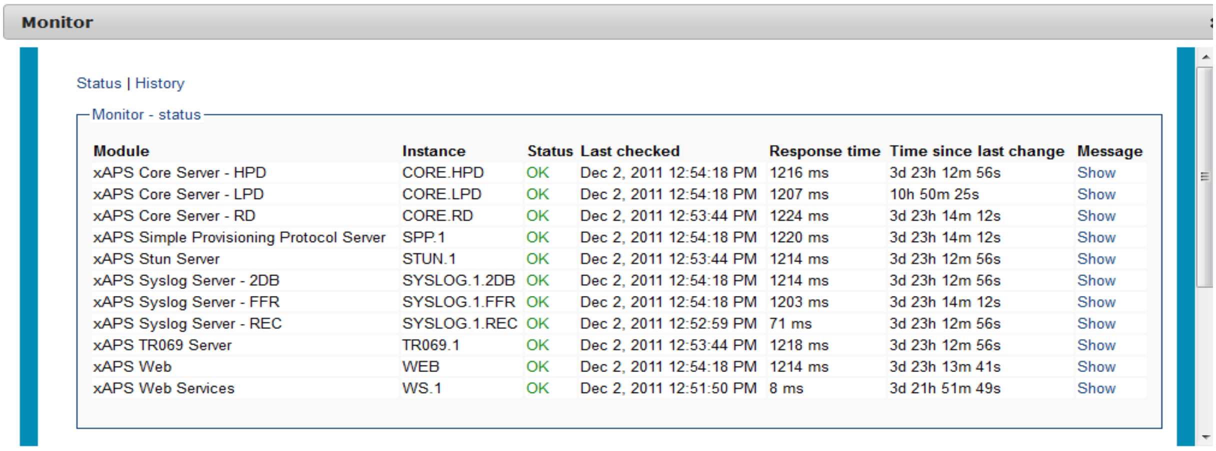
Permissions: No permission is defined.

NPA201E-Pingcom All profiles

Decide user name and password. In modules you specify which pages to have access to. Then add permissions to various Unit Types and Profiles. If no Unit Type is specified, the user have access to all Unit Types. If no Profile is specified, all profiles within the Unit Type is accessible.

4.2 Monitor

The monitor page (found on the top-menu) provides a status page showing all the modules in Fusion. Check xaps-web.properties to point to the correct URL of the monitor module. If modules report error on the page, check xaps-monitor.properties to get correct URLs.



Module	Instance	Status	Last checked	Response time	Time since last change	Message
xAPS Core Server - HPD	CORE.HPD	OK	Dec 2, 2011 12:54:18 PM	1216 ms	3d 23h 12m 56s	Show
xAPS Core Server - LPD	CORE.LPD	OK	Dec 2, 2011 12:54:18 PM	1207 ms	10h 50m 25s	Show
xAPS Core Server - RD	CORE.RD	OK	Dec 2, 2011 12:53:44 PM	1224 ms	3d 23h 14m 12s	Show
xAPS Simple Provisioning Protocol Server	SPP.1	OK	Dec 2, 2011 12:54:18 PM	1220 ms	3d 23h 14m 12s	Show
xAPS Stun Server	STUN.1	OK	Dec 2, 2011 12:53:44 PM	1214 ms	3d 23h 12m 56s	Show
xAPS Syslog Server - 2DB	SYSLOG.1.2DB	OK	Dec 2, 2011 12:54:18 PM	1214 ms	3d 23h 12m 56s	Show
xAPS Syslog Server - FFR	SYSLOG.1.FFR	OK	Dec 2, 2011 12:54:18 PM	1203 ms	3d 23h 14m 12s	Show
xAPS Syslog Server - REC	SYSLOG.1.REC	OK	Dec 2, 2011 12:52:59 PM	71 ms	3d 23h 12m 56s	Show
xAPS TR069 Server	TR069.1	OK	Dec 2, 2011 12:53:44 PM	1218 ms	3d 23h 12m 56s	Show
xAPS Web	WEB	OK	Dec 2, 2011 12:54:18 PM	1214 ms	3d 23h 13m 41s	Show
xAPS Web Services	WS.1	OK	Dec 2, 2011 12:51:50 PM	8 ms	3d 21h 51m 49s	Show

4.3 Help

The top menu has a Help section. This will give you help for the current page you're accessing. Help is also found throughout the pages (shown by small question-mark-signs).

4.4 The context bar

The context bar that sits on top of every page in Fusion Web is a toolbox for selecting objects and for quick navigation. It is meant to make it easier to select the appropriate Unit Type, Profile etc, because it will be displayed in the same way on all pages.

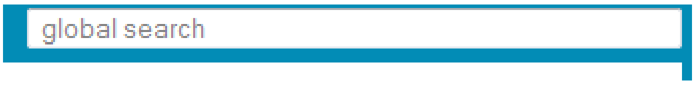
Because the various pages does not need to implement their own logic for selecting these objects and by always knowing where to look, the work flow and page layout can be a lot more efficient. The context bar is also the primary place to look for alternative actions on the current page. With all this in mind the operator or administrator can focus on the task at hand.

In its simple explanation the only functionality contained within the context bar is a variable number of selects, that when selected introduces other selects or object pages that may provide a list of shortcuts that is then displayed in the context bar as a drop-down select.

4.5 Search

4.5.1 Global search

Fusion has several ways to locate units. First is the global search located in the upper right corner.

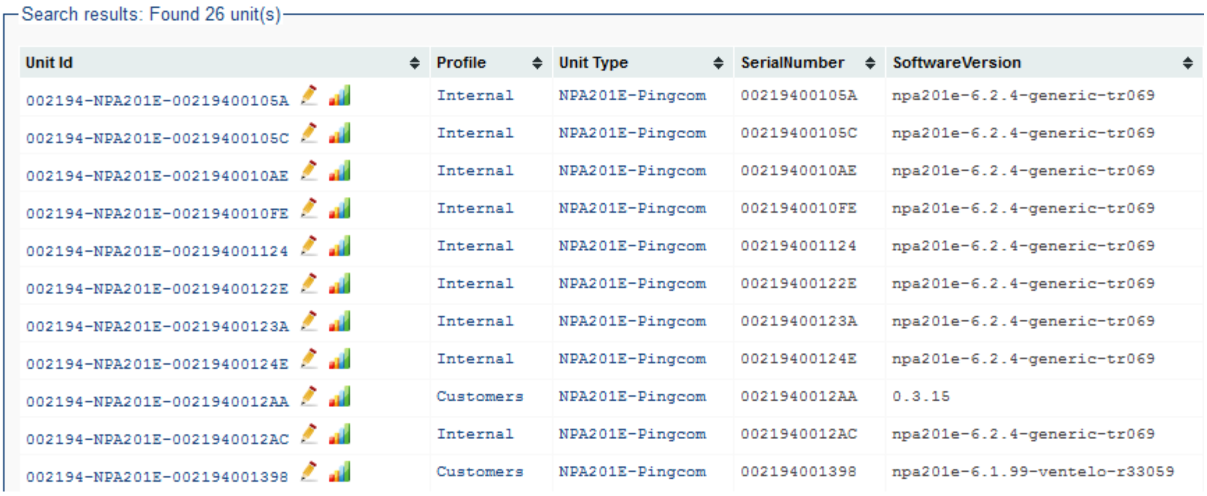


This search will search for a Unit Parameter value or a Unit Id across all Unit Types in the system. This means that if you search for a number, let's say "888", all devices that has this number either as part of a password, phone number, Unit Id, will be listed.

4.5.2 Context search

This search works exactly the same way as global search, but only within the given context (Unit Type and/or Profile). You'll find the search field in the context bar. If a Unit Type is chosen, the search output will show more information (see Displayable Flag in

Parameters chapter), otherwise only a list of Unit Ids that match will be listed. Here's an example of extended listing:

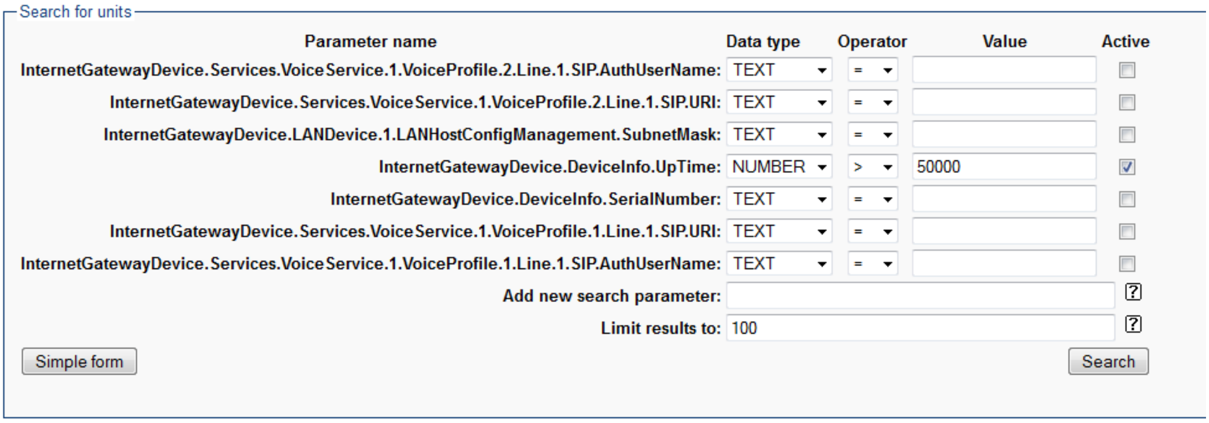


Search results: Found 26 unit(s)

Unit Id	Profile	Unit Type	SerialNumber	SoftwareVersion
002194-NPA201E-00219400105A	Internal	NPA201E-Pingcom	00219400105A	npa201e-6.2.4-generic-tr069
002194-NPA201E-00219400105C	Internal	NPA201E-Pingcom	00219400105C	npa201e-6.2.4-generic-tr069
002194-NPA201E-0021940010AE	Internal	NPA201E-Pingcom	0021940010AE	npa201e-6.2.4-generic-tr069
002194-NPA201E-0021940010FE	Internal	NPA201E-Pingcom	0021940010FE	npa201e-6.2.4-generic-tr069
002194-NPA201E-002194001124	Internal	NPA201E-Pingcom	002194001124	npa201e-6.2.4-generic-tr069
002194-NPA201E-00219400122E	Internal	NPA201E-Pingcom	00219400122E	npa201e-6.2.4-generic-tr069
002194-NPA201E-00219400123A	Internal	NPA201E-Pingcom	00219400123A	npa201e-6.2.4-generic-tr069
002194-NPA201E-00219400124E	Internal	NPA201E-Pingcom	00219400124E	npa201e-6.2.4-generic-tr069
002194-NPA201E-0021940012AA	Customers	NPA201E-Pingcom	0021940012AA	0.3.15
002194-NPA201E-0021940012AC	Internal	NPA201E-Pingcom	0021940012AC	npa201e-6.2.4-generic-tr069
002194-NPA201E-002194001398	Customers	NPA201E-Pingcom	002194001398	npa201e-6.1.99-ventelo-r33059

4.5.3 Support/Search page

To find a unit, go to the search page (located under Support menu choice). The simple search, which is default, works the same way as the Context search. However, on this page you can use the Advanced search.



Search for units

Parameter name	Data type	Operator	Value	Active
InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.2.Line.1.SIP.AuthUserName:	TEXT	=		□
InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.2.Line.1.SIP.URI:	TEXT	=		□
InternetGatewayDevice.LANDevice.1.LANHostConfigManagement.SubnetMask:	TEXT	=		□
InternetGatewayDevice.DeviceInfo.UpTime:	NUMBER	>	50000	☑
InternetGatewayDevice.DeviceInfo.SerialNumber:	TEXT	=		□
InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.1.SIP.URI:	TEXT	=		□
InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.1.SIP.AuthUserName:	TEXT	=		□
Add new search parameter:				
Limit results to:	100			

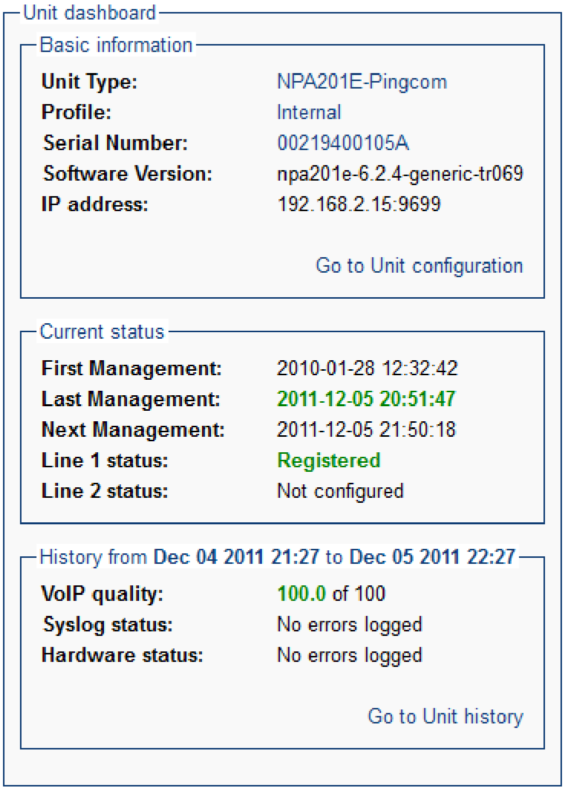
In the example above you may search for a number of parameters, choose data type (NUMBER or TEXT) and operator (>,>=,=,<,<=,<>) and value. The value may contain these special characters:

* (asterix)	: 0 or more character of any kind
_ (underscore)	: 1 character of any kind
^ (circumflex)	: Start of string
$ (dollar)	: End of string

If the parameter is not found in the list, you can add it directly or add a Searchable Flag on the Unit Type Parameter (see Parameters chapter). Using this search page you can make very specific searches and hopefully cover most needs. Furthermore, this search page can also be a valuable analysis tool. Later we will cover Group functionality, and it will be shown that a group is in fact doing exactly the same thing as this search.

4.6 Unit Dashboard

When you click on a Unit Id from the Unit listing on the Search page you should usually come to a Unit Dashboard. The Unit Dashboard contains a summary of the important states of the device in terms of provisioning/management, software version, VoIP service and hardware status.



Unit dashboard

Basic information

Unit Type:	NPA201E-Pingcom
Profile:	Internal
Serial Number:	00219400105A
Software Version:	npa201e-6.2.4-generic-tr069
IP address:	192.168.2.15:9699

Go to Unit configuration

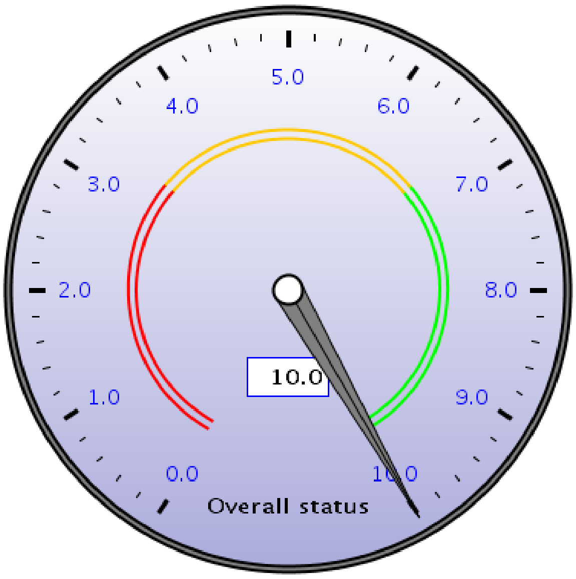
Current status

First Management:	2010-01-28 12:32:42
Last Management:	2011-12-05 20:51:47
Next Management:	2011-12-05 21:50:18
Line 1 status:	Registered
Line 2 status:	Not configured

History from **Dec 04 2011 21:27** to **Dec 05 2011 22:27**

VoIP quality:	100.0 of 100
Syslog status:	No errors logged
Hardware status:	No errors logged

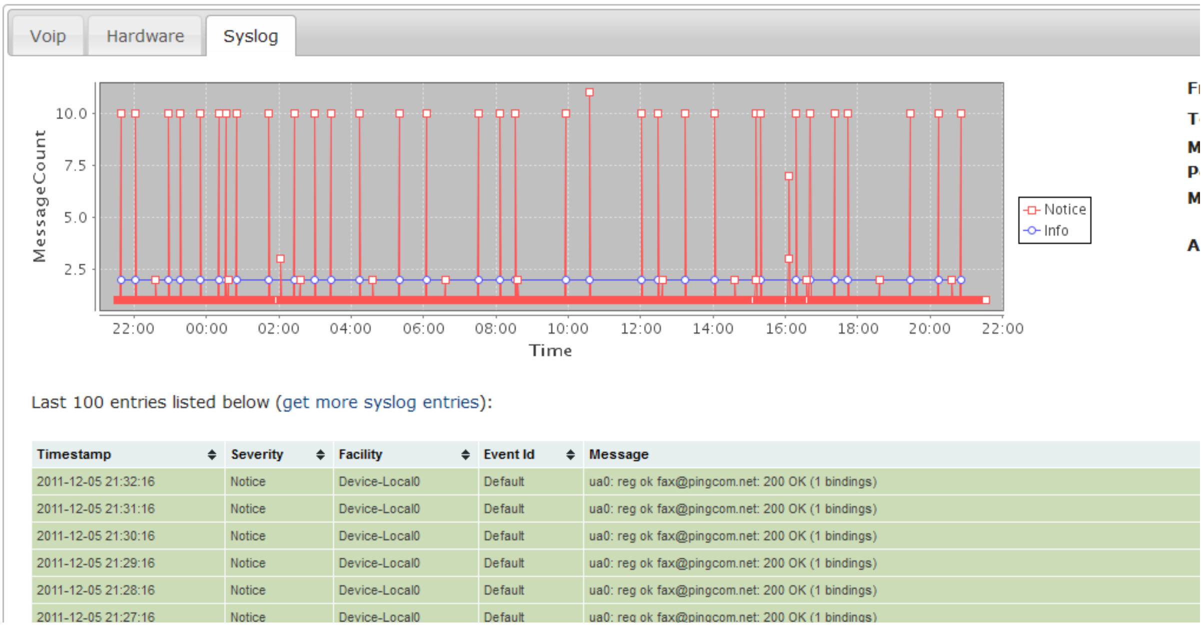
Go to Unit history



The green text and top score on the speedometer all indicates a good status. The yellow color signifies a warning, while the red signals error. The overall status speedometer will summarize all the states of the device, to give the Fusion Operator a quick overview of the situation. The text on the right will indicate which part of the system may be the cause of a problem (if any).

4.7 Unit History

From the dashboard it's possible to navigate to the Unit Configuration (described in later chapters) and Unit History. The history provides an overview of the various components of a device, such as hardware history and VoIP history. The syslog for this particular device is also shown.



Last 100 entries listed below (get more syslog entries):

Timestamp	Severity	Facility	Event Id	Message
2011-12-05 21:32:16	Notice	Device-Local0	Default	ua0: reg ok fax@pingcom.net: 200 OK (1 bindings)
2011-12-05 21:31:16	Notice	Device-Local0	Default	ua0: reg ok fax@pingcom.net: 200 OK (1 bindings)
2011-12-05 21:30:16	Notice	Device-Local0	Default	ua0: reg ok fax@pingcom.net: 200 OK (1 bindings)
2011-12-05 21:29:16	Notice	Device-Local0	Default	ua0: reg ok fax@pingcom.net: 200 OK (1 bindings)
2011-12-05 21:28:16	Notice	Device-Local0	Default	ua0: reg ok fax@pingcom.net: 200 OK (1 bindings)
2011-12-05 21:27:16	Notice	Device-Local0	Default	ua0: reg ok fax@pingcom.net: 200 OK (1 bindings)

The idea is that an Fusion Operator should get at quick overview of the device/Unit using the dashboard, and then move into the history to get more insight into the details.

5 Brief introduction of concepts & startup

In Fusion Web you can create, update, delete and administrate a pool of Units. The Units are all associated with a Profile and all Profiles is associated with a Unit type. These concepts is a crucial part of how you operate the web. For more information about these basic concepts of Fusion, read [1].

Imagine that the Fusion Administrator are at square one. There are no Units, no Unit types and no Profiles. What the Fusion Administrator should do now is to first to create a new Unit type. This new Unit type will hold the parameter definitions for all Profiles created within that Unit type.

Secondly, create a new Profile. This Profile will hold a set of shared values that all Units created within the Profile will share.

Then the Fusion Administrator creates a new Unit within the Profile. This Unit is logical representation of a physical CPE. This representation allows an operator to change the CPE configuration, like SIP settings etc. Usually you would either import or auto detect the Units, not create them one by one in Fusion Web, so in this document you will only see dummy Units for the tutorials.

When you have a pool of Units, you can make a new Group. A Group is a selection of Units based on their parameter values, and can further be used to create a Job. A Job will make a controlled and safe changes on a number of Units, be it a Software upgrade or configuration change. Jobs provide a safer change than what you could achieve by provisioning Units by setting their new values on their Profile.

On the left side menu the orange color signals the chosen menu item. Depending upon what rights you have been given as a user of Fusion Web, you might not see all possible menu items. Communicate with your Fusion Administrator to update your security rights. If need be, the Fusion Administrator must install a certificate to be able to use some of the features, like the Reporting module.

A detailed explanation for most of all of the functions can be found in [1]. To get a better understanding of Fusion Web, it is strongly suggested that you first read the referred document. The Monitor page is explained in [3].

In this document you will be guided through a set of tutorials for the most interesting use cases in Fusion.

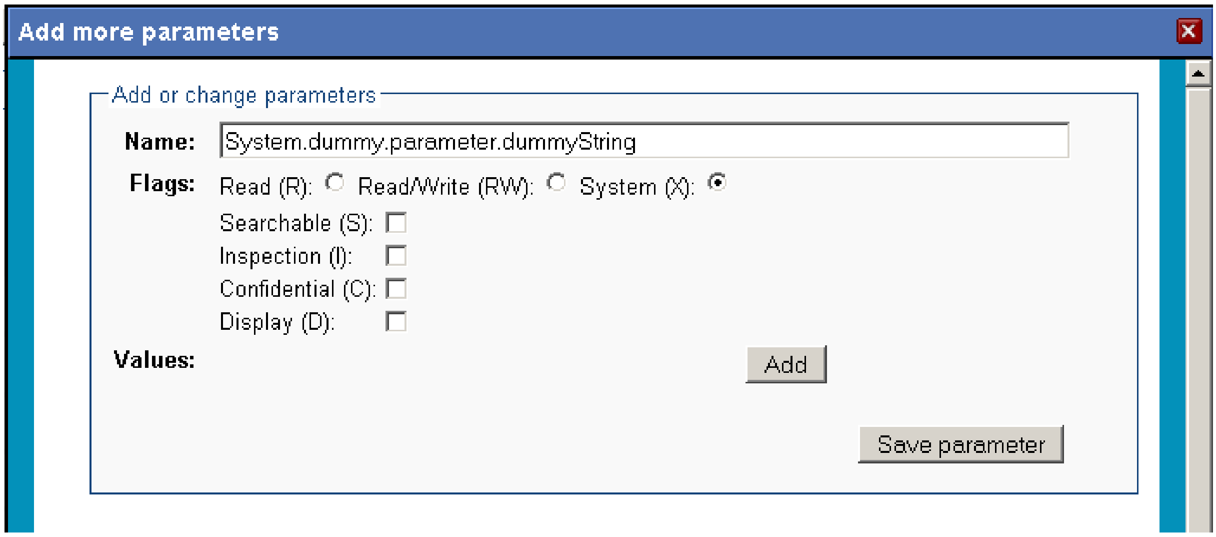
6 Parameters concept

The **only** thing a devices offer to a provisioning server is a set of parameters that can be read and/or written. (This is not entirely true, a device can also upgrade it's firmware and restart/reset, but you get the point:-) Fusion treats all parameters the same way, that is in a generic way. So no matter what kind of device you're using, or whichever TR-specifications it support, Fusion can handle it - because in the end is all about a set of parameters being read/written.

Because of this approach you will often see lists of parameters on various pages, ranging from Unit Type and Unit to Group and Job. Everywhere the list of parameters is crucial to give you the maximal flexibility and ability to provision the device as you see fit.

For a parameter to exist in the system, a Unit Type parameter must be defined. Think of this as the parameter definition for the device, in other words this is how Fusion knows what kind of "possibilities" the device offers. A parameter has a name and it has some flags indicating what type of parameter it is.

Navigate to the Unit Type configuration page (you must have created a Unit Type) and click "Add more parameters" in the "Select action" drop-down. A window will pop up for you to create a new Unit Type Parameter.



Add more parameters

Add or change parameters

Name: System.dummy.parameter.dummyString

Flags: Read (R): ○ Read/Write (RW): ○ System (X): ●

Searchable (S): □

Inspection (I): □

Confidential (C): □

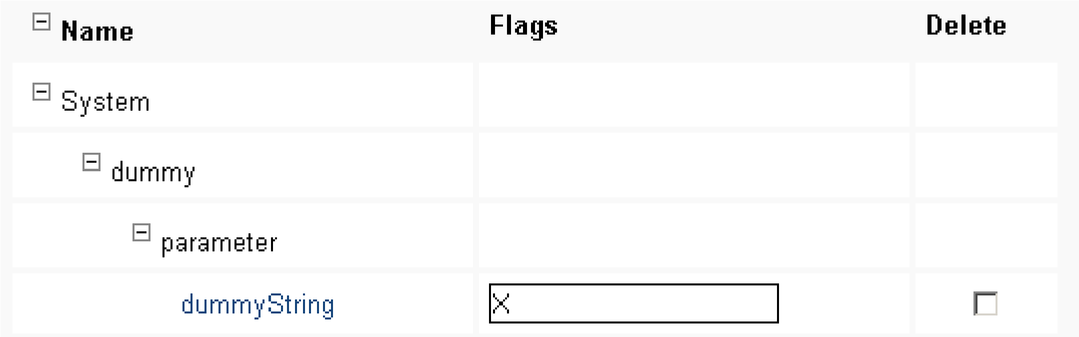
Display (D): □

Values:

The following rules apply to the name of a parameter:

- If the parameter is to be read/written to the device it must have the exact same name as the parameter in the device. That translates into a parameter starting with "InternetGatewayDevice." or "Device.". Example: Device.DeviceInfo.Uptime Usually the set of parameters in the device is "discovered" by the TR-069 server, so you don't have to do the work of creating all Unit Type parameters manually.
- If the parameter is a Fusion/system/server-side parameter, it's usual to prefix it with "System.". All necessary system parameters are created/updated once a Unit Type is created or modified.
- Do not insert space or strange characters
- Use dots to separate words/hierarchy. Example: System.dummy.parameter.dummyString

This dotted notation makes it possible to make a tree-structured view of the parameters. The above example translates to the image on the next page.



⊟ Name	Flags	Delete
⊟ System		
⊟ dummy		
⊟ parameter		
dummyString	X	□

6.1 Unit Type Parameter Flag

6.1.1 Mandatory flags

If a parameter is a CPE/device parameter, it must have the flag R or RW. For all system parameters you must specify the X flag. If you fail to specify the X flag on system parameter, the provisioning server will try to retrieve system parameters from the device, which will result in huge performance loss (you will be notified in the logs from the TR-069 server).

6.1.2 Optional flags

The (S)earchable flag is set when you want to be able to search for a specific parameter in the Advanced section of the Support/Search page. Otherwise searches are performed across all parameter values for all devices in the Unit Type or Profile specified.

The (D)isplayable flag is set whenever you want to display this particular parameter in the Support/Search page listing of units. However, this parameter will not be displayed unless you have explicitly chosen a Unit Type in the context navigation bar. The D flag cannot be combined with C or I flags.

The (C)onfidential flag is set to hide confidential parameters from logs and also to some degree in this web interface. However, you will still be able to see the parameter value in the configuration page. The other important usage of this flag, is for the TR-069 server know when to expect blank values returning from the device. Passwords are normally never returned from the device, and because of the compare algorithm in the TR-069 server, it might prompt it to transmit the password again and again. This is both a security risk (although very little if you run SSL) and unnecessary, and it creates warnings in the logs. The warnings will tell you when you probably need to add the C-flag.

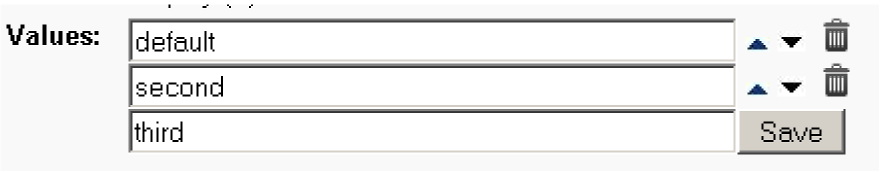
The (I)nspection flag is specified on those parameters that you want to inspect in case of a customer call, but never want to provision. The idea is that provisioning is something you do to a limited set of parameters, but when a customer calls and have some problems, you might be interested in 100 more parameters. These parameters are always deleted from Fusion DB as soon as Inspection mode is closed.

When the (A)lways-read flag is specified, the parameter will always be read from the device. To understand why this is necessary, think of all the parameters that a device can support; it can be thousands. You don't want all those parameters read into the Fusion DB, even if they have the R-flag set. Adding the A-flag makes sure that the parameter is read and stored in the Fusion DB. The A-flag cannot be combined with RW, X or I flags.

You might also see a (M)onitor flag. The flag can only be specified on R-flag parameters. The usage of monitoring flags will trigger a syslog message to be sent, containing the value of the parameter, prefixed by the Unit Type Parameter Number (internal number in Fusion DB). This is not something a Fusion Administrator would use, but it is used in conjunction of TR-reports (mentioned in Repeatable Job chapter and in the Shell documentation).

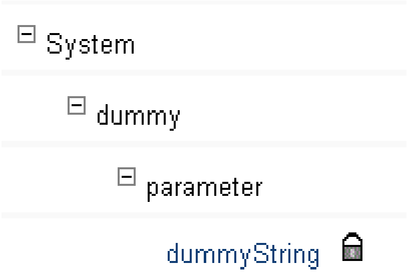
6.2 Unit Type Parameter enumerated values

In the "Add more parameters" window previously shown, you can add enumerated values to the parameter, that will show up as a drop-down menu with default values on unit, profile, group and job parameters. You change the default values and move them up and down. The value at the top is the default selected value.



Values: default, second, third

If you have added enumerated values you will see a "lock" icon beside the parameter name.

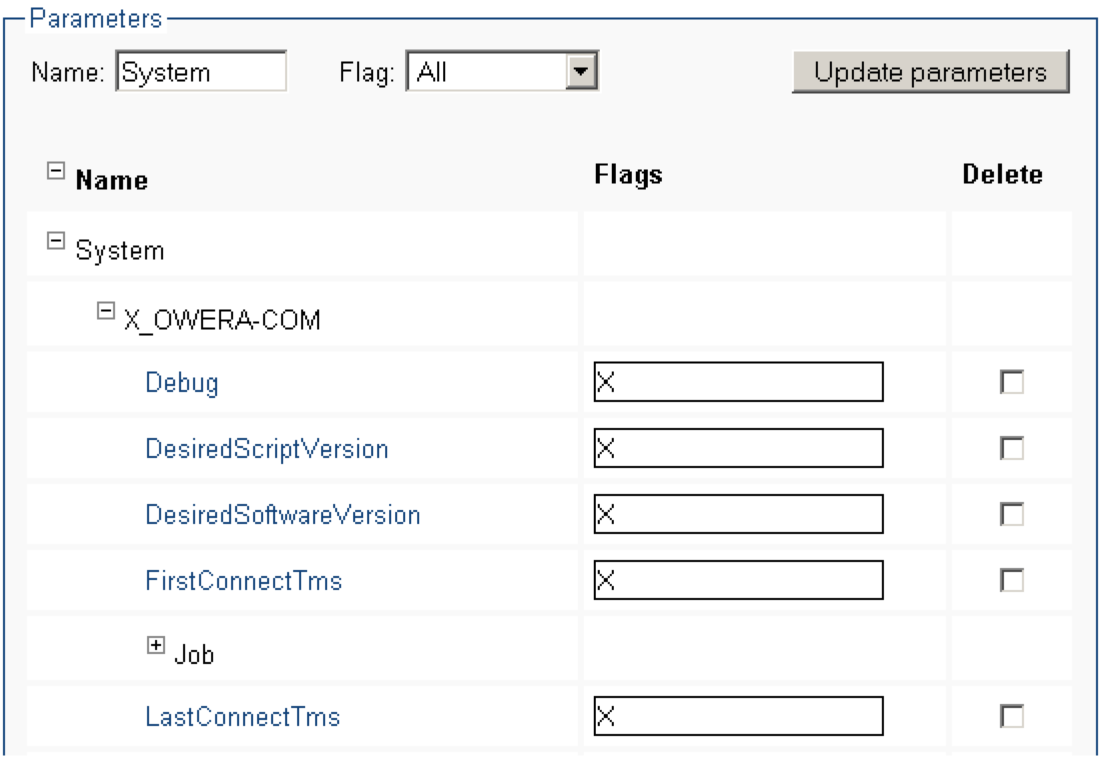


6.3 Parameter Filter & Parameter change

One of the nice features of the web interface which is worth mentioning is that the parameter listings can be collapsed and expanded as needed to hide any set of parameters. This is extremely useful from the users perspective when only a certain set of parameters is of concern. By entering “System” in the Name filter input field on the top, you will only show parameters which contains the word “System”. The flag drop-down filter can be use in a similar way to only see parameters with a specific flag.

To collapse/expand just click the minus/plus icons. Clicking the header “Delete” will check all parameters for deletion. This goes for Profile and Unit too. See figure 3.

Fig 3: Create/Update/Delete Unit Type parameters:



Parameters

Name: System Flag: All

⊟ Name	Flags	Delete
⊟ System		
⊟ X_OWERA-COM		
Debug	X	□
DesiredScriptVersion	X	□
DesiredSoftwareVersion	X	□
FirstConnectTms	X	□
⊞ Job		
LastConnectTms	X	□

You will see this parameter list many times, in various contexts. Always the same: filters and a possibility to collapse/expand. Furthermore you are able to do a lot of changes at once. You can change many flags or delete a lot of parameters. Then when you are satisfied, press the button on the top or the bottom of the page.

6.4 *Other parameter types*

So far Unit Type Parameters have been discussed. The other types of parameters are

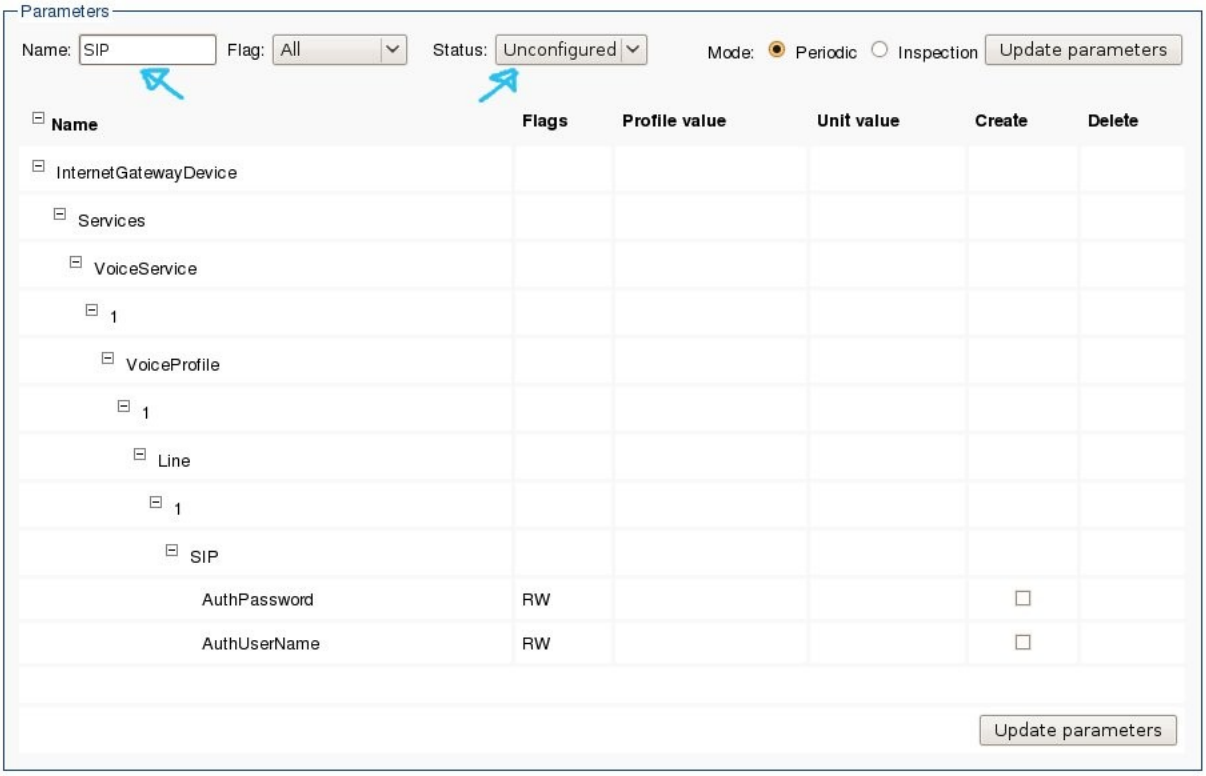
- Unit Parameter
- Profile Parameter
- Group Parameter
- Job Parameter

All these parameters is in fact also a Unit Type Parameter, but the difference is that they also have a value attached to the parameter. And this value applies to whatever context the parameter is specified in (Unit, Profile, etc..). Group and Job parameters also have some extra properties, which will be discussed in later chapters.

6.5 *How to set parameters*

If the operator needs to configure some SIP parameters, he can use the filter section to look these up. However, the filter section needs to explained. By default, when no unit parameters are defined, 'Status' is set to 'All' which means that both 'Unconfigured' and 'Configured' unit parameters are displayed at the same time. On the second hand, if some unit parameters are configured, then the status will be set 'Configured'. If SIP parameters is not set and there are other unit parameters configured, you will not be able to see the SIP parameters unless you change 'Status' to 'All' or 'Unconfigured'.

Lets try to search for the SIP parameters. First, in the 'Name' filter enter 'SIP'. Next, select 'Unconfigured' in drop down menu 'Status'. You will then get a display like this (if you have <u>not</u> configured SIP settings for this device, that the parameters are unconfigured):

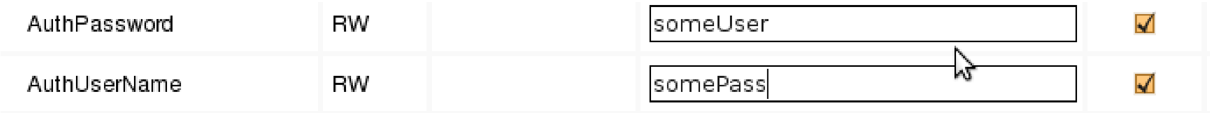


Parameters

Name: SIP Flag: All Status: Unconfigured Mode: ● Periodic ○ Inspection

⊟ Name	Flags	Profile value	Unit value	Create	Delete
⊟ InternetGatewayDevice					
⊟ Services					
⊟ VoiceService					
⊟ 1					
⊟ VoiceProfile					
⊟ 1					
⊟ Line					
⊟ 1					
⊟ SIP					
AuthPassword	RW			□	
AuthUserName	RW			□	

Now you will have to click the create check-boxes and enter the user name and password:



AuthPassword	RW		someUser	☑
AuthUserName	RW		somePass	☑

Finally, hit the “Update parameters” button to save your newly created settings. If you do not hit this button after changing the parameters they will not be saved. The button is placed both at the top and at the bottom of the table. Please note that you can search for other parameters and create/edit those before you hit the update button. This enables creating and editing a lot of parameters without the need to scroll through the whole list of parameters. By default you will not be presented with a confirmation when you hit the update button, but this is possible to turn on. Ask your administrator if that sounds interesting.

7 The quick setup

You can now set up a basic provisioning for your devices. First make sure your device is discovered, so that you have a Unit Type fully populated with Unit Type Parameters. Then, in the default profile add all the units you want to provision. Specify Profile parameter values for all common values, and specify the Unit parameters values for all specific to each physical device (ex: passwords, user name). Connect the devices to the provisioning server and the system should provide your devices with the correct configuration. At this point you have the most basic provisioning up and running. You will probably very quickly expand the system with more profiles, but apart from that many customers can work quite well with this basic setup. (Actually this must include a Web Service integration from the CRM system, otherwise it will be too tedious.)

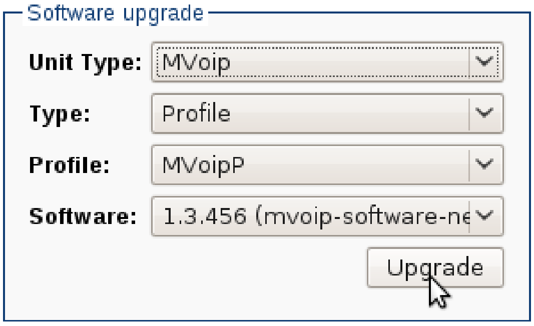
8 Software upgrade

Units and Profiles can be upgraded to another software version through an upgrade wizard. This upgrade wizard does not do the actual upgrade itself but changes the desired software version parameter. The devices connecting to Fusion provisioning servers will change/upgrade upon contact. Therefore a software upgrade on a profile may take days or even weeks to complete, since not all device connect regularly.

If you want to upgrade a Unit or Profile to another Software version, you are able to do so in the "Select action" drop-down on each of those pages. You will get a new window where you can select the desired Software version, and then click upgrade.

A green message should inform you that it went OK.

Fig 5.1: Upgrade Profile:



Unit Type: MVoip

Type: Profile

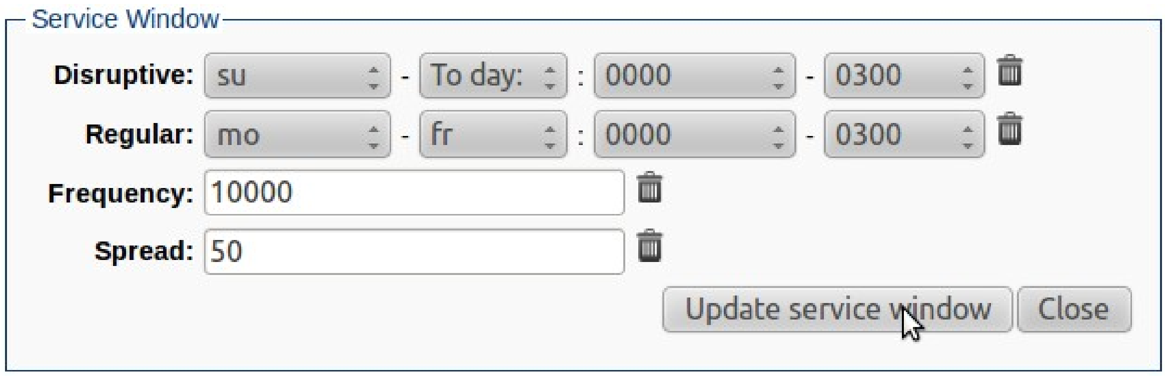
Profile: MVoipP

Software: 1.3.456 (mvoip-software-ne

9 Service window & Provisioning Frequency

A Service Window defines when a Unit can be provisioned. The ACS will inform the CPE when it can connect based on this service window. Fusion provides two Service Windows. The Regular SW is used for all changes which do not disrupt the services on the CPE, while Disruptive SW is for all changes that do disrupt services on the CPE. As long as no disruptive change has been specified (like a Software upgrade), the CPE will connect according to the Regular SW, that is within the time window specified.

If you want to configure Service Window for your Profile (for all Units within this Profile), you are able to do so in the "Select action" drop-down. After selecting from day, to day, from and to time and frequency and/or spread, clicking “Update service window” will set the correct parameters in the Profile.



Disruptive: su - To day: : 0000 - 0300

Regular: mo - fr : 0000 - 0300

Frequency: 10000

Spread: 50

The Frequency tells you how often the CPE will connect to Fusion. Default is 7, which means 7 times a week. Spread denotes the percent of randomization of the interval between each connect. Default setting is 50, which means that if the device is supposed to connect 7 times a week, and that the Regular SW is open all day and all week, the interval may be from 12h to 36h. The spread is useful to avoid synchronized CPE connects (meaning high load on the server) in the event of a large power outage.

A configuration change can be both Disruptive and Non-disruptive (Regular), but Fusion cannot possibly know how the CPE will react. In that case, you must turn to Jobs to make the configuration change, because a Job can be associated with a Service Window. For other changes, Fusion will automatically choose the correct Service Window (like Software Upgrade, Factory Reset and Reboot).

10 Provisioning Modes

10.1 Periodic mode

The normal operation of Fusion provisioning is to be in "periodic mode". This means that the device will connect to the server as often as requested by the server through the parameter called "PeriodicInformInterval". Upon connect, the device will go through a normal provisioning session, checking for changes and jobs, reading and writing data. You can see which mode the device is in at the Unit Configuration page (at the top of the parameter list).

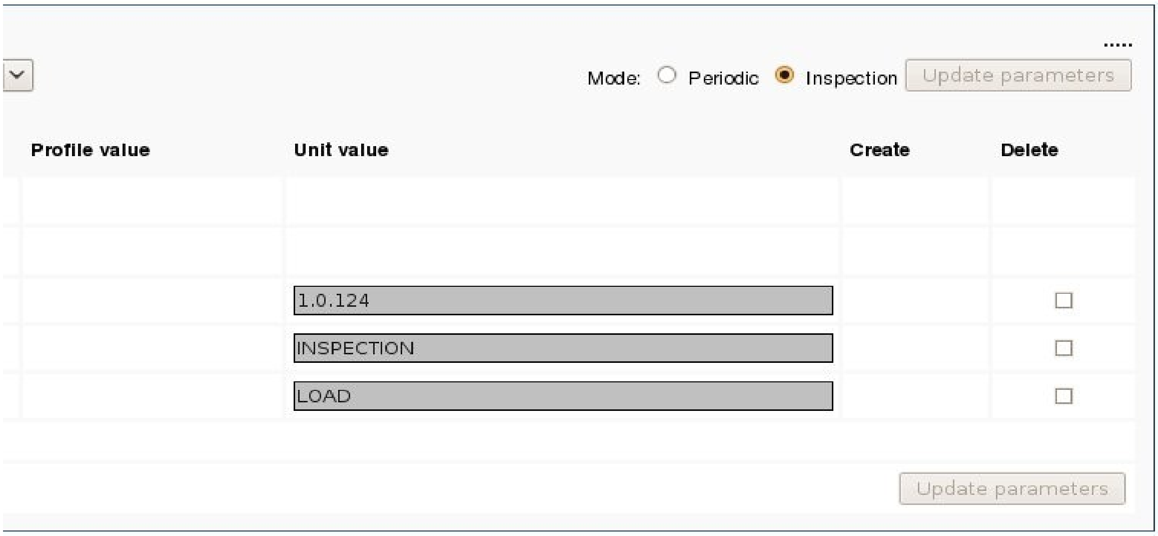
10.2 Inspection mode

The inspection mode is extremely useful for the provisioning of an individual Unit. The idea is that you may inspect parameters which aren't under standard provisioning, that is: not visible in the Fusion system. You can set a Unit Type parameter flag to 'I' on those parameters of special "Inspection" interest. Then, in inspection mode, you're able to examine more data from the device than usually available to you.

Lets say you want to inspect a Unit. You are the support personnel, someone is calling in to get technical help with his or her device. You identify the customer and looks up the Unit. At this point the Unit is running in periodic provisioning mode, that means it will provision normal within the given service window. But you want it to connect to the server now and give you all the necessary parameters to identify the problem the customer has given you. On the Unit page, in the Parameters section, you'll find three radio buttons for Mode: **Periodic, Inspection** and **Kick**. If you hit the Inspection button, the page will refresh and wait until the server has processed the request. Normally this takes up to 15-60 seconds.

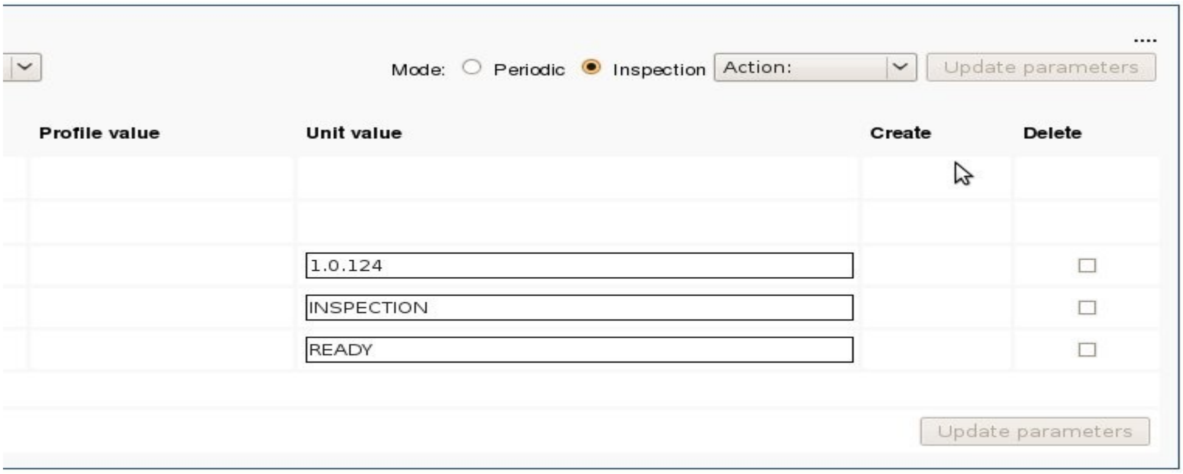
When the device has been taken into Inspection mode, a drop down list will appear beside the two radio buttons where Inspection now is selected. This drop down list contains the possible actions you could do, **Retrieve data** and **Perform change**. At this point the server has already retrieved the parameters, so you can start reviewing/editing them straight away. When you need to send the updated parameters to the device, select Perform change from the drop down list and the server will try to send the updated parameters to the device.

Fig 10: Operator is waiting for the server to enter inspection mode:



Mode: ○ Periodic ● Inspection

Profile value	Unit value	Create	Delete
	1.0.124		□
	INSPECTION		□
	LOAD		□



Mode: ○ Periodic ● Inspection

Profile value	Unit value	Create	Delete
	1.0.124		□
	INSPECTION		□
	READY		□

The operator can now inspect the Unit. When the operator is finished editing the parameters, choose Perform change from the drop down menu "Action:" will save the parameters and the ACS will try to update the CPE accordingly.

If for some reason it is impossible to return back to Periodic mode (could happen if the Fusion STUN Server is not working), you can delete the parameters ProvisioningMode and ProvisioningState.

10.3 Kick mode

Fusion also provides a third option (apart from Periodic and Inspection) which is Kick. This is a third radio button (not shown in the screen shots above). When you click on this button, Fusion will issue a kick to the CPE, which must return to perform a provisioning within 30 seconds. This is useful when you have some changes on the server which you need to apply on the CPE right away.

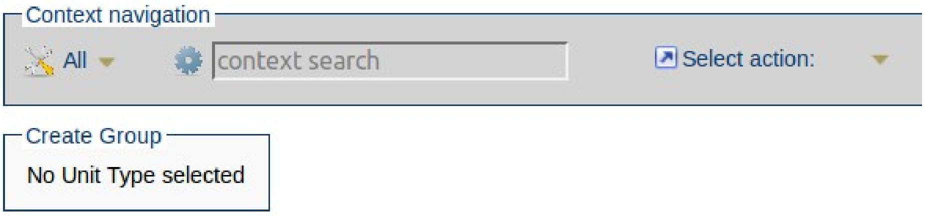
11 Group tutorial

In the Group page, you can add/change/delete/inspect a particular Group. In order to create a Group, you have to select the Unit type, enter a Group name, and add a description. For this tutorial, create two new Unit type parameters for your Unit type:

```
System.X_OWERA-COM.Country
System.X_OWERA-COM.Region
```

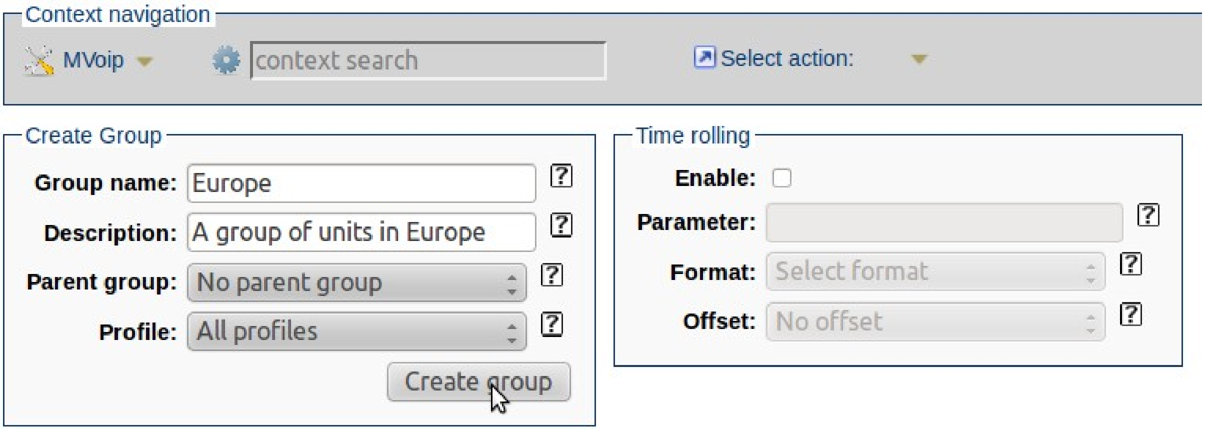
11.1 Simple group

Select Management → Group → Create Group



No Unit Type selected

Select the appropriate Unit Type in the first select within the context bar that currently has the text "All". If it is already selected then you do not have to worry about selecting it and the screen will look like the one below. Ignore the "Time rolling" settings for now.



Group name: Europe

Description: A group of units in Europe

Parent group: No parent group

Profile: All profiles

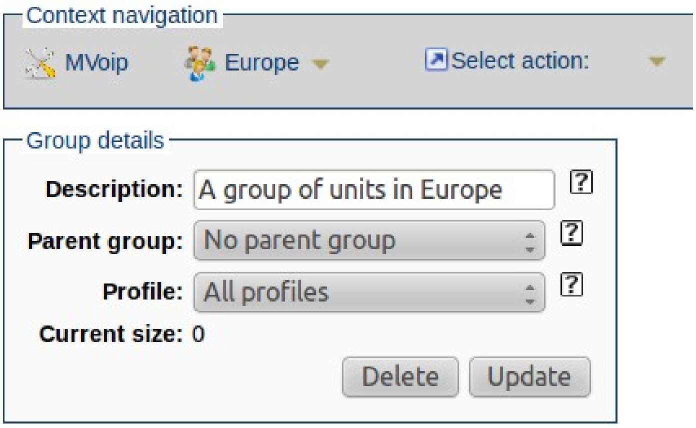
Enable: □

Parameter:

Format: Select format

Offset: No offset

Type in the Group name and description and hit "Create group". You have now created a group which contains all units within this Unit Type. You should see the Current Size be equal to the number of units in the Unit Type.



Context navigation

MVoip Europe Select action:

Group details

Description: A group of units in Europe

Parent group: No parent group

Profile: All profiles

Current size: 0

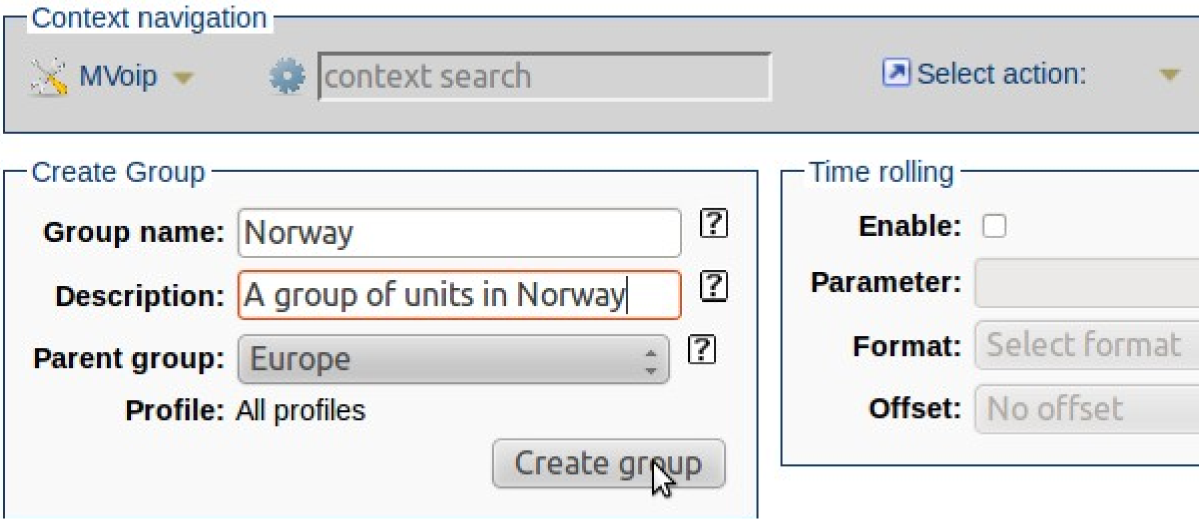
Delete Update

11.2 Group hierarchy

It is possible to create a hierarchy in the Group structure, by setting a parent Group. The Profile selection will then be inherited from the parent Group, and cannot be changed. If a Group has not defined a Profile, the selection is *All Profiles,* that is all Units within the given Unit type.

Select Management → Group → Create Group

Select Europe as "Parent group" (assuming you have created such a group), and then input the name and description, and hit "Create group". Note that when choosing a parent group you cannot change the profile, since it will be automatically inherited from the parent group.



Context navigation

MVoip context search Select action:

Create Group

Group name: Norway

Description: A group of units in Norway

Parent group: Europe

Profile: All profiles

Create group

Time rolling

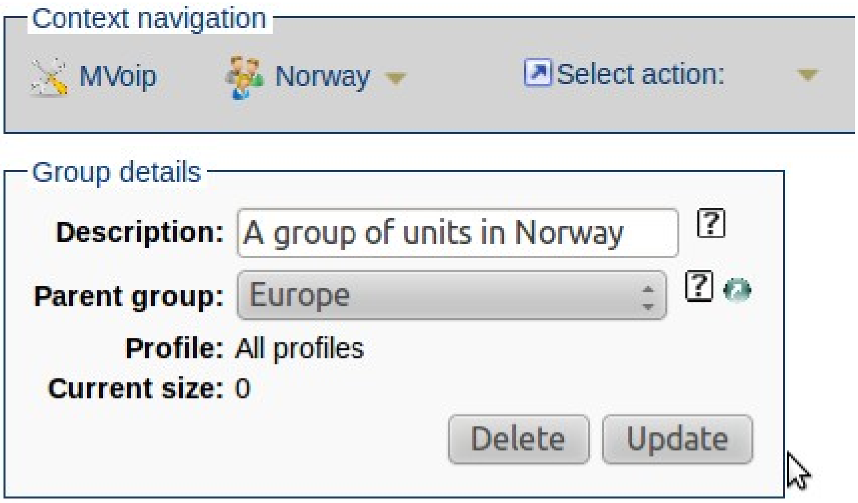
Enable: □

Parameter:

Format: Select format

Offset: No offset

You will get something like the screen below:



Context navigation

Group details

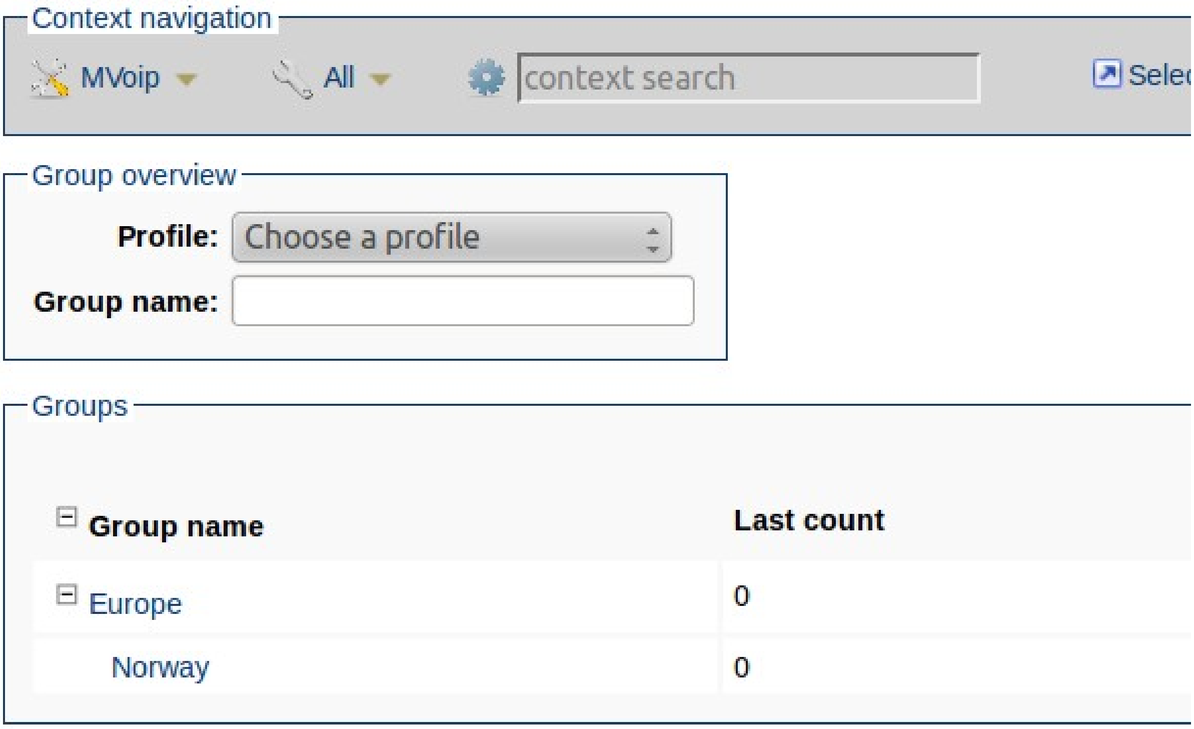
Description: A group of units in Norway

Parent group: Europe

Profile: All profiles

Current size: 0

Notice above that there is a small green shortcut icon at the right side of the parent group drop down that links directly to the parent group. Also notice that you are now not able to change the profile for the Group since it is inherited automatically. Since the Group has a parent it will be displayed in the Group Overview page as a sub group under Europe as seen on the next page.



Group overview

Profile: Choose a profile

Group name:

Groups

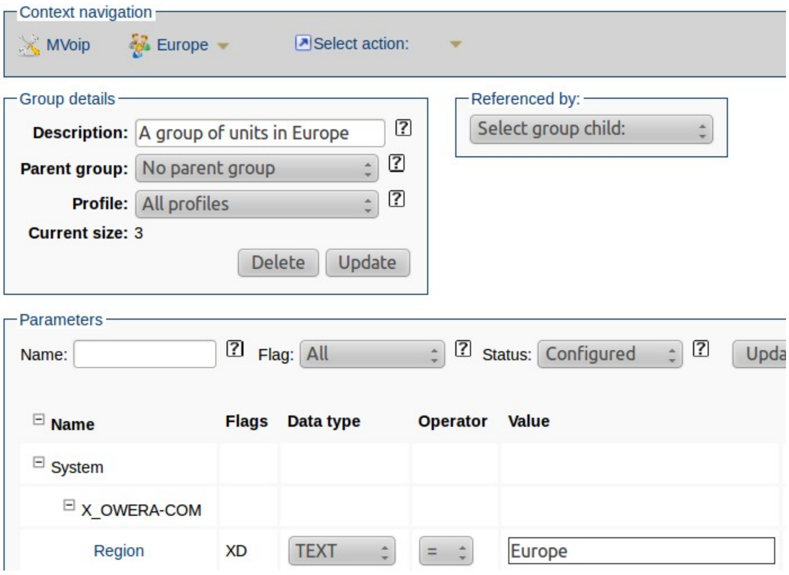
Group name	Last count
⊟ Europe	0
Norway	0

You can filter Groups based on their name and Profile. If you have a lot of top level Groups and dependent children, you would then use this filter to only display a certain a subset of all the Groups.

11.3 Group parameters

Before going through this tutorial it is important to have a pool of units in the Unit Type you are working on. In our example, we have added three dummy units to test with.

The *current size* field in the group Europe below denotes the number of Units that are currently part of the Group. It can in some cases take some time to load the Group due to the calculation of this number of Units. As you can see there is three units that matches the group parameter Region.


Context navigation
MVoip Europe Select action:

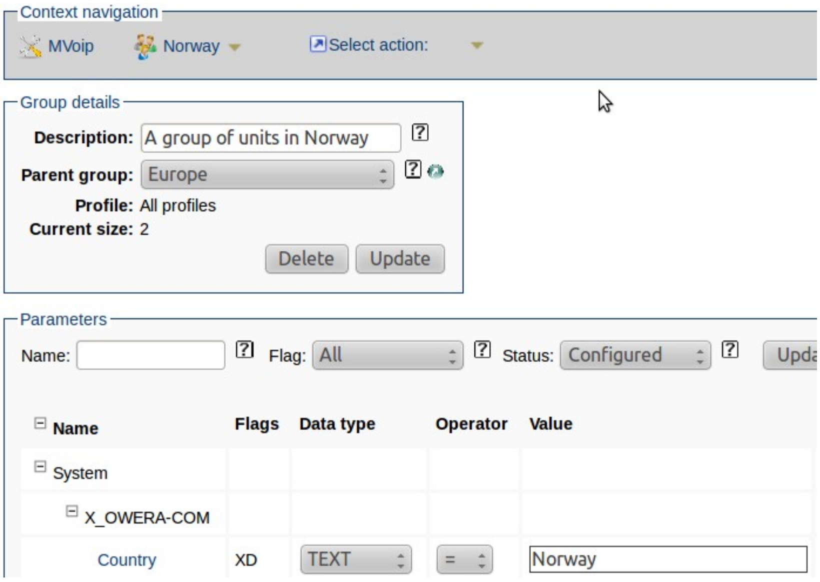
Group details
Description: A group of units in Europe
Parent group: No parent group
Profile: All profiles
Current size: 3

Referenced by:
Select group child:

Parameters
Name: Flag: All Status: Configured

Name	Flags	Data type	Operator	Value
System				
X_OWERA-COM				
Region	XD	TEXT	=	Europe

When we take a look at the group Norway we can see that its size is two. This is because we have on purpose configured two of the three units to be within Norway. You can see a list of units that matches this group (or any) in "Select action:".


Context navigation
MVoip Norway Select action:

Group details
Description: A group of units in Norway
Parent group: Europe
Profile: All profiles
Current size: 2

Parameters
Name: Flag: All Status: Configured

Name	Flags	Data type	Operator	Value
System				
X_OWERA-COM				
Country	XD	TEXT	=	Norway

The child group Norway inherits the parameters from the parent group Europe, and thus if it was thousands of units in Fusion and the Europe group was configured to only contain three units, the Norway group would only have access to those three units for filtering. The rules for search parameter value is the same as for regular search covered in chapter 4. The "Select action" offers a link to the search page, with the group-parameter search criteria.

11.4 Time rolling groups

Time rolling groups is easy to understand, once you understand the use cases which triggered this feature:

1. We want to monitor an occurrence of a certain syslog message over time. This report of monitoring can be viewed in the report system of Fusion, just choose the correct time rolling group.
2. We want to start a specific job to set a debug-flag or turn off a debug-flag once a certain syslog message have been emitted. The job is connected to the time rolling group.
3. We want to cleanup or change something for a group of device depending on a timestamp.

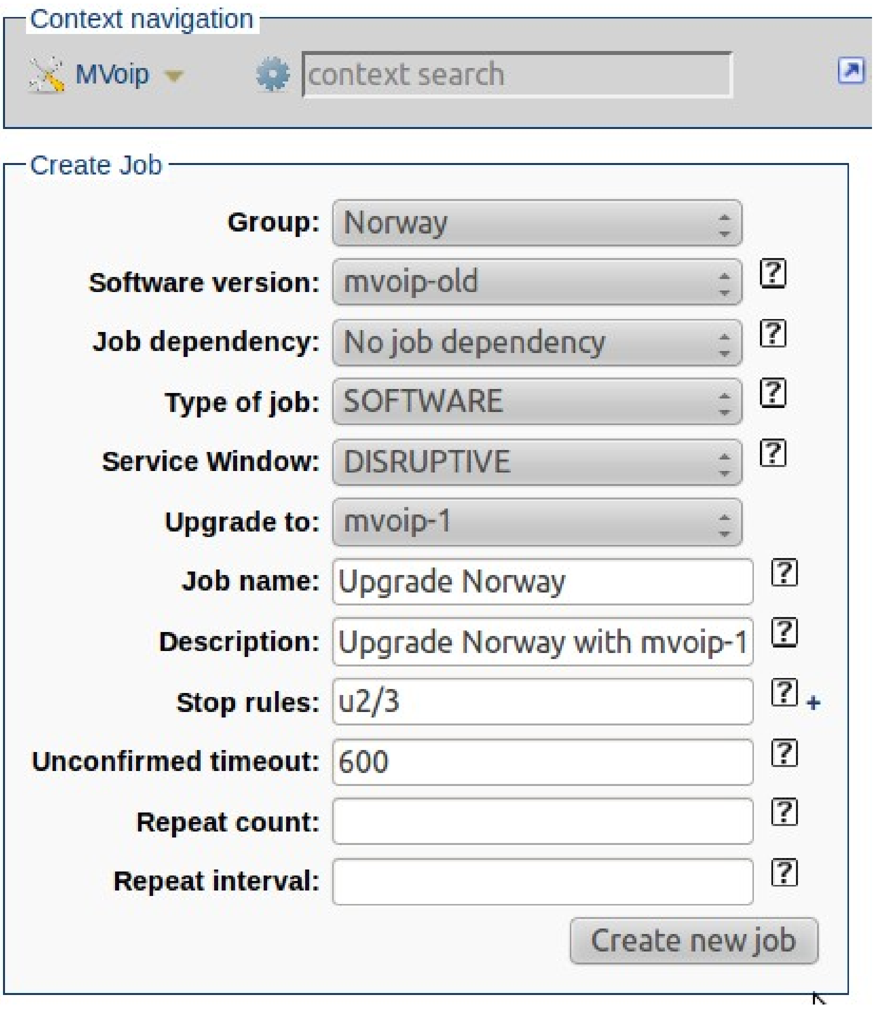
A time rolling group is a group where one specified group parameter is updated either every hour or every day with the time of that hour or that day. If an offset (number of days) is specified, the time stamp is calculated as the current time plus the offset. In short, we have a group that changes it's search criteria every now and then.

This doesn't make a whole lot of sense unless coupled with a syslog event (you can read more about this in a later chapter). A syslog event can be set up to synchronize with a group parameter - usually the time rolling parameter - and copy it to the unit which emitted the particular syslog message. In this way, we're able to mark units emitting certain syslog messages with a time stamp. The group will "capture" these units in the brief time the parameters are the same, in other words on the same hour or the same day.

The idea of "offset" is to be able to create some cleanup jobs connected to some cleanup groups (with offset set to for example 1 or 3 days). In this scenario you must create two groups: One with an offset and one without. The one with an offset is coupled to a Syslog Event which set the future timestamp on the unit. The other group is coupled to a Job which will find the group of previously updated group of devices some days later. Then the job can perform some cleanup operation.

12 Job tutorial

A Job is the action that you want to perform on a Group. It is important to remember that a Job is connected to one Group only. To create a Job, you should select the appropriate Unit type, Group, name and then a description. It is possible to move Units to a specified Profile, in addition to the ordinary Job routines. This can be configured in the following interface. In this tutorial we will upgrade all Units in Group Norway to a new Software. We want the Units to match Software version mvoip-old.



Create Job

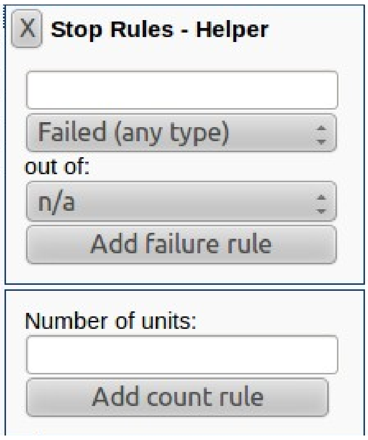
Group:	Norway
Software version:	mvoip-old
Job dependency:	No job dependency
Type of job:	SOFTWARE
Service Window:	DISRUPTIVE
Upgrade to:	mvoip-1
Job name:	Upgrade Norway
Description:	Upgrade Norway with mvoip-1
Stop rules:	u2/3
Unconfirmed timeout:	600
Repeat count:	
Repeat interval:	

Jobs can have a dependency, and this means that the Jobs will have to wait for the Job dependency to complete. Because of this you can make structures of Jobs that will run in sequence.

You can also set stop rules for the Job, and this is made easy with a GUI that pops up when you hit the plus sign on the right side of the input field for the stop rules. These settings will help you to define when the Job should stop.

An example of this is "stop when 1 Unit has had an Unconfirmed Failed Situation out of the last 3 Unit Jobs". When you hit the Add failure rule it will be converted to u1/3 in the text field.

You can also tell the system how many Units that should be processed before the Job is complete. And for how long time the Job should run, in hours. These tools give you full control over how the Job will stop.



X Stop Rules - Helper

Failed (any type)

out of:

n/a

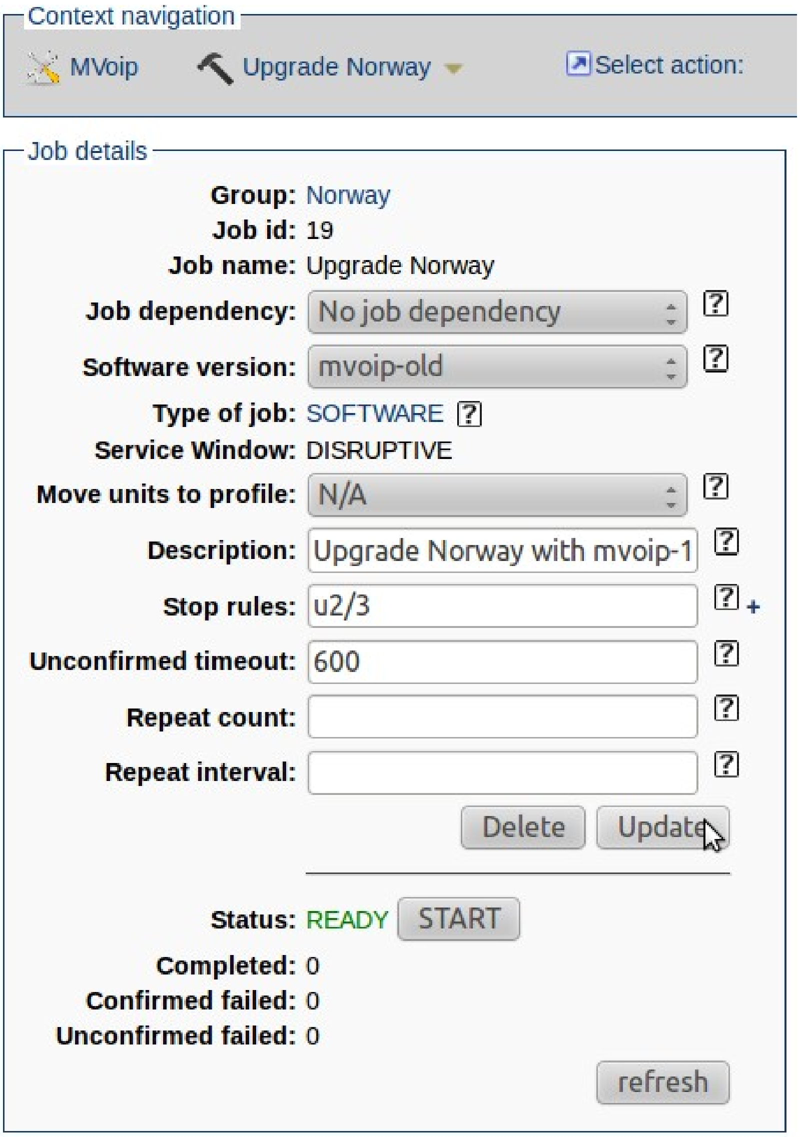
Add failure rule

Number of units:

Add count rule

To start the Job, hit the START button. When the job has started you may hit the STOP button (equivalent to PAUSE), and you can START again.

Note that you cannot change any parameters set if the Job has been started, so make sure you have everything set correct before you start the Job.



Context navigation

MVoip Upgrade Norway Select action:

Job details

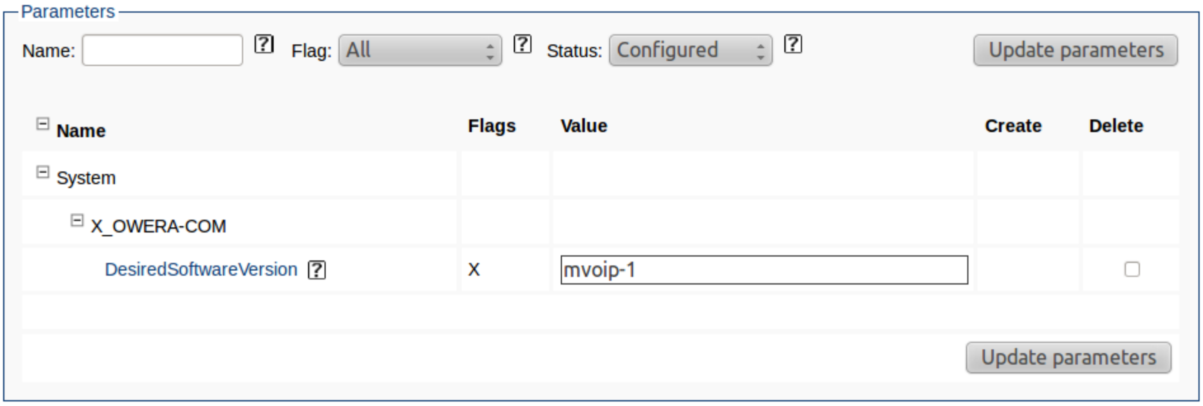
Group:	Norway
Job id:	19
Job name:	Upgrade Norway
Job dependency:	No job dependency
Software version:	mvoip-old
Type of job:	SOFTWARE
Service Window:	DISRUPTIVE
Move units to profile:	N/A
Description:	Upgrade Norway with mvoip-1
Stop rules:	u2/3
Unconfirmed timeout:	600
Repeat count:	
Repeat interval:	

Delete Update

Status:	READY START
Completed:	0
Confirmed failed:	0
Unconfirmed failed:	0

refresh

In our test case, we wanted to upgrade all Units in Norway to a new Software version mvoip-1. Choose the software version from the software version drop down list. You can see in the Job parameters that the parameter has been set correctly. Other parameters (than DesiredSoftwareVersion) cannot be set on a SOFTWARE job.



Name: Flag: All Status: Configured

Name	Flags	Value	Create	Delete
System				
X_OWERA-COM				
DesiredSoftwareVersion	X	mvoip-1		□

12.1 Various Job types

A job can be of many types. Each one has a specific purpose and usage.

12.1.1 CONFIG

A configuration job is the most typical job, where a set of parameters are specified and applied on the device as the device connects to the server.

12.1.2 SOFTWARE

A software job upgrades the software of the device upon connect. Upload the software into the files section (as SOFTWARE type) and specify the software name in the job.

12.1.3 SCRIPT

A script job transmits a proprietary script to the device upon connect. This is usually something done to overcome the limitations of the TR-069 stack in the device (some changes might not be possible through plain TR-069 parameters). Upload the script into the files section (as SCRIPT type) and specify the script name in the job.

12.1.4 RESTART

A restart job will issue a Reboot command to the device.

12.1.5 RESET

A reset job will issue a Factory Reset command to the device.

12.1.6 KICK

A kick job issues a kick to a whole group of units. The kick will trigger the devices to connect to the server immediately, thus triggering a change of the devices quickly. This job is run server-side, so the job starts as soon as you have hit the Start-button. The kick interval is controlled in the xaps-stun.properties file, but defaults to 1 second between each kick. Thus a group of 3600 devices will take approximately 1 hour to kick start.

12.1.7 TELNET

A telnet job issues a telnet script to the devices in the group. Upload the telnet script into the files section (as SCRIPT type) and specify the script name in the job. This job is run server-side, so the job starts as soon as you have hit the Start-button. Check out xaps-spp.properties for configuration on how to control the number of parallel telnet sessions to devices.

For this job to work a set of parameter must be specified. The parameters can be specified either on the job or unit or profile or unit (which is also the precedence order). These parameters all share the same prefix "System.X_OWERA-COM.Telnet.". The parameters are:

1. IPAddress - The IP address of the device. The address must be a public IP. If no address is specified, the public IP address stored in parameter System.X_OWERA-COM.Device.PublicIPAddress is used instead.
2. Port - The port number default to 23 if not specified.
3. Username - Optional, if necessary for the telnet login
4. Password - Optional, if necessary for the telnet login

The login procedure to the device is not very robust, since telnet access is not highly standardized. Therefore, if the device does not ask for a "login" or "username" or "password" with exactly these phrases (they are still optional, but if username is wanted it *must* be asked for using "username" or "login"), the login procedure will fail.

As soon as a connection is established and login procedure is completed, the script will run at the telnet device. Usually this script will perform changes on the device which were not possible to achieve using regular provisioning. But in addition, the Fusion Telnet Job also offers the possibility to retrieve information from the running of the telnet script. The method goes like this:

Make a Unit Type Parameter starting with "TelnetDevice." prefix. The rest of the parameter name should be something to identify the information, for example MemoryConsumption. The unit type parameter flag must be "X". This parameter will be created/overwritten on the unit and populated with the data coming from the telnet session. Furthermore, create the same Unit Type parameter name, but add a _PP postfix to the parameter name. Thus in this example you will have two parameters:

TelnetDevice.MemoryConsumption
TelnetDevice.MemoryConsumption_PP

The latter property must be set (on job, unit or profile) and must contain a regular expression. If the regular expression contains a set of parenthesis, the parenthesis marks the actual content that you will find/extract. An example of such a regular expression could simply be

Memory-consumption: ([^,]*)

Which will populate the MemoryConsumption with whatever comes after "Memory-consumption:", and before ",".

You can have as many of these TelnetDevice parameters as you like.

But this is not all, you can also specify certain AbortConditions to the script, which will abort the script run and avoid a situation where the script does changes which it shouldn't have done. One or more AbortConditions can be specified by creating one or more parameters with the prefix "System.X_OWERA-COM.Telnet.AbortCondition." and the postfix "_PP". Specify a regular expression here as well, and if the script encounters a match, the script will abort and the job will be marked as CONFIRMED FAILED (important for the stop rule previously mentioned).

12.1.8 SHELL

A shell job performs a shell script upon contact with the device. Thus this job is triggered by the connection of the device. Upload a shell script into the files section (as SCRIPT type) and specify the name of the script in the job. Check out xaps-tr069.properties for configuration on how to control the number of parallel shell sessions.

The process of this job is that the device uploads it's read-only parameters to the server upon contact. Then the shell script is executed, and finally the end result of the parameter settings (of the read-write parameter) is sent back to the device. You may view this kind of job as an extended version of the normal CONFIG job, with the difference that you have the ability to apply some complex logic in the provisioning "engine". This is something you may use in the most complex cases, where regular provisioning falls short. One use case has been to change the ACS-username upon contact of the server, create a new unit and return the new ACS-username to the device.

12.2 Repeatable job

A job can be repeatable if a repeat counter is specified. The main use case for this is twofold:

- Being able to restart a device on a regular basis
- Being able to retrieve monitor-data from a device on a regular basis

For this reason, the repeat interval is not supposed to be spread, like regular provisioning (check the Service Window chapter). The repeat count number cannot be set to infinity; the highest number allowed is 2147483647 (2^{31}-1). If a repeat interval is not specified, it defaults to 86400 seconds (= 24h). The repeat interval cannot be shorter than 120 seconds. The repeatable jobs will respect the service window and the way it will do that is to skip the executions of the job whenever it falls outside the service window. The result of that is that the job will still maintain it's steady schedule (every hour for example), and not skewed/spread by the service windows. The intervals between the jobs can however be prolonged if specified to be very short, and if many jobs are setup to run at the same time.

To make jobs to extract monitor data to populate the TR-reports available in Fusion, please look into the Shell documentation, since the operation of setting up such specific monitoring jobs are pretty complicated.

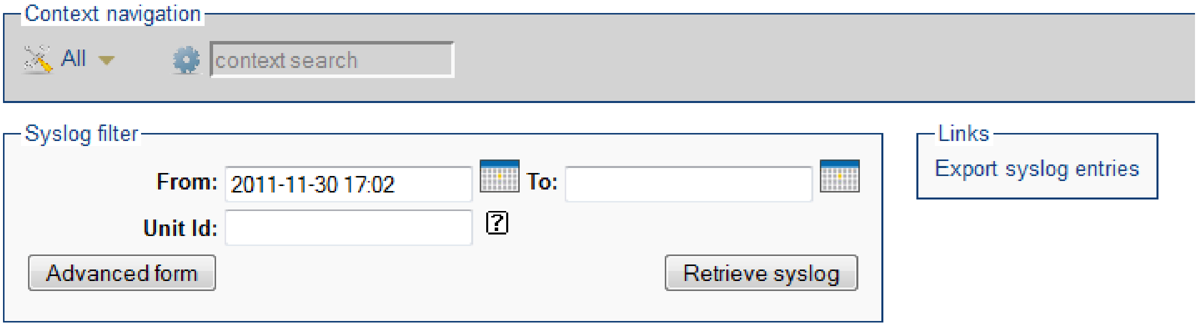
13 Syslog and Syslog events

13.1 Syslog message matching

Fusion has put a lot of effort into making good use of the syslog messages usually emitted from the device. The first thing we need to make sure of is how to connect the messages coming from the device, with the correct unit in Fusion Database. The messages can be marked with the MAC/Serialnumber of the device. If so, the Syslog Server must understand how to identify the number. This is to be configured in the xaps-syslog.properties. If no MAC/Serialnumber is found, the only available information in the message to identify the syslog-emitting device is the IP address. The Syslog Server will then try to match MAC/Serialnumber/IP-address with Unit information in then Fusion DB. If there is a match, the syslog messages will be linked to the correct Unit. For this reason it is important that the (A)lways-Read Unit Type Parameter Flag is specified for those parameters than contains Serialnumber or MAC. The public IP address is always stored in a System parameter.

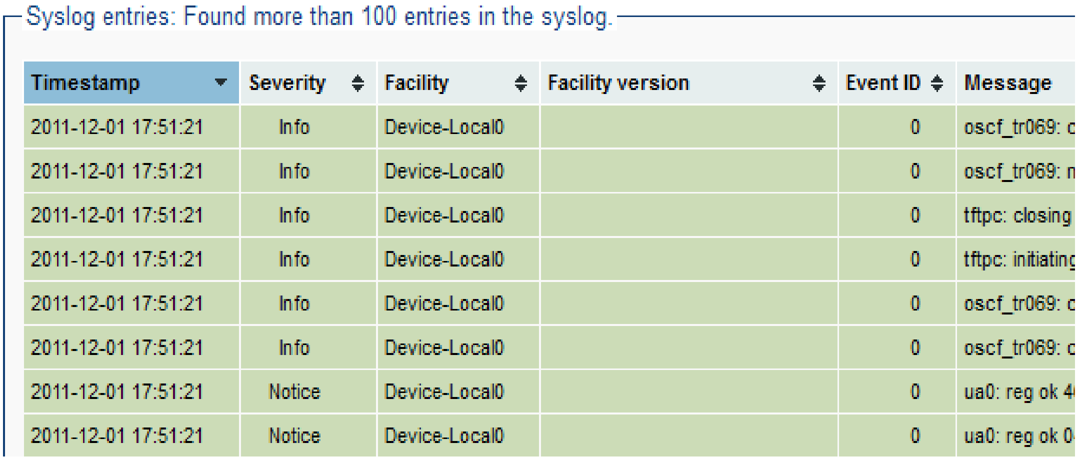
13.2 Simple search

Navigate to the syslog page. Make sure the Context Bar above is set to "All".



From:	2011-11-30 17:02
To:	
Unit Id:	

The From time is always set to yesterday (24h since now), in case there is a long time since any messages were received. The To field is purposely empty, meaning "To eternity". You can use the calendar-icons to choose other days and hours (try clicking on the hours and move the mouse!), or edit the fields manually. When satisfied, hit "Retrieve syslog". You will then retrieve the 100 newest syslog messages that satisfy the time and Unit id criteria. The data can be exported using the link "Export syslog entries".



Syslog entries: Found more than 100 entries in the syslog.

Timestamp	Severity	Facility	Facility version	Event ID	Message
2011-12-01 17:51:21	Info	Device-Local0		0	oscf_tr069: c
2011-12-01 17:51:21	Info	Device-Local0		0	oscf_tr069: n
2011-12-01 17:51:21	Info	Device-Local0		0	tftpc: closing
2011-12-01 17:51:21	Info	Device-Local0		0	tftpc: initiating
2011-12-01 17:51:21	Info	Device-Local0		0	oscf_tr069: c
2011-12-01 17:51:21	Info	Device-Local0		0	oscf_tr069: c
2011-12-01 17:51:21	Notice	Device-Local0		0	ua0: reg ok 4
2011-12-01 17:51:21	Notice	Device-Local0		0	ua0: reg ok 0

13.3 Columns

The columns in the output are:

Timestamp: This is the time when the Fusion Syslog Server received the message, not when it was emitted from the device. The reason for this is that device clocks may not be correct and even if they are, but devices are spread across timezones, it may confuse the user of Fusion Web.

Severity: The syslog standard defines 7 levels of severity:

DEBUG - lowest level, will contain all kinds of information
INFO - information of some interest
NOTICE - information of high interest
WARN - indicates an issue, but not a problem
ERROR - indicates a problem, but only for one device/module - not
CRITICAL - system failure
ALERT - all systems failed

Facility: A facility identifies the type of syslog emitter. All modules in Fusion may log into the syslog database, but because of incomplete naming transition you will find them with names like "xAPS TR069" or "xAPS Web". Other facilities of interest are "Device-Local0" which is often used to identify a CPE, but this may vary from one CPE to another.

Facility-version: All facilities are installed with a version, which is very important in an analysis.

Event-ID: An Event ID is short for "Syslog Event ID". You may create certain patterns (explained later) to identify certain messages and then mark these with an ID.

Message: The real content

User: If facility is "xAPS Web" this would constitute the user of the application, and it is mostly for Web that this is interesting (if you want track some changes).

Host name: The syslog message contain a field for the host emitting the message. Not used too often. Could contain an IP address.

IP address: The public IP address of the syslog facility, as seen from the Syslog Server

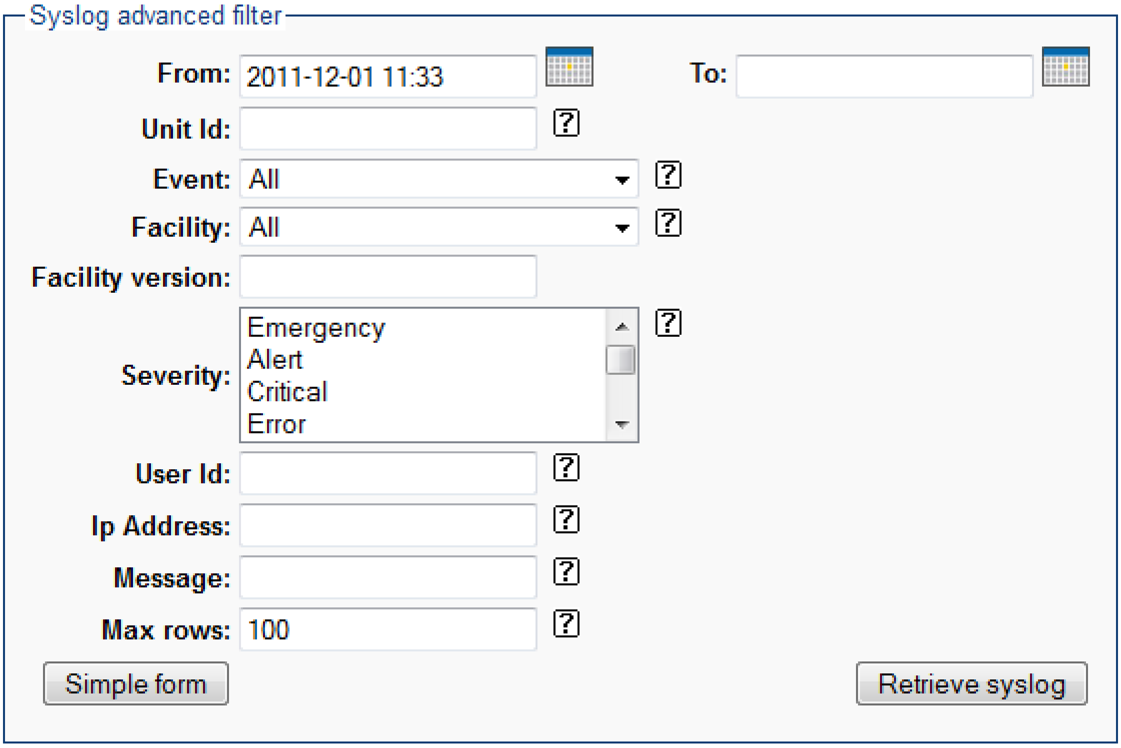
Unit ID: The Unit, if applicable

Profile: The Profile, if applicable

Unit Type: The Unit Type, if applicable

13.4 Filtering

Press the "Advanced" button, to get a list of all filters that can be applied. The list of filters matches pretty much the list of columns, except for Unit, Profile and Unit Type (which you can filter by changing the Context Navigate Bar on top) and the number of rows in the result.



Syslog advanced filter

From: 2011-12-01 11:33

To:

Unit Id:

Event: All

Facility: All

Facility version:

Severity: Emergency, Alert, Critical, Error

User Id:

Ip Address:

Message:

Max rows: 100

Some fields allow strings to be entered. Then you can add special characters to control the search. These are:

* (asterix)	: 0 or more character of any kind
_ (underscore)	: 1 character of any kind
^ (circumflex)	: Start of string
$ (dollar)	: End of string
! (exclamation)	: Negation, only to be used at the beginning of filter.
| (pipe)	: Logical or, means the ability to search for many strings.

Examples on how to use:

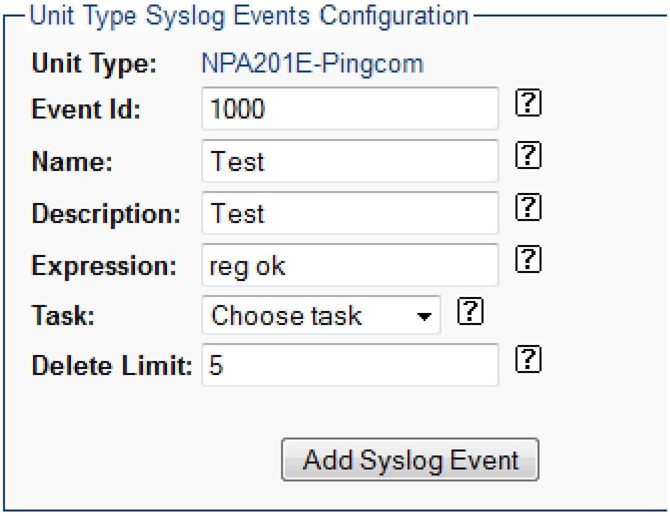
- IP address starts with 101.202. and ends with .56:
  101.202.*.56
- Facility version is 6.x.3 where x can be one digit (not 6.10.3)
  6._.3
- Everything but messages that includes "problem"
  !problem
- Everything except messages ending with "foobar"
  !foobar$
- All messages that includes "foo" and "bar"
  foo|bar

Tip: Enclosing a string without wildchars, with ^ and $, can speed up searches considerably.

14 Syslog Event

Go to the Unit Type Configuration page of one of your Unit Types. In the "Select Action" drop-down you'll find a link to "Manage syslog events".

The idea of syslog events is to perform some kind of action based upon the content of the message. To create a syslog event, you must first decide upon a syslog event id. This id is a number, which must be 1000 or above. Then make a name for the event and the pattern in the message to match.



Unit Type Syslog Events Configuration

Unit Type:	NPA201E-Pingcom
Event Id:	1000
Name:	Test
Description:	Test
Expression:	reg ok
Task:	Choose task
Delete Limit:	5

In the example above we have specified the pattern to be "reg ok". In this pattern matching you can use standard regular expression, which gives you great flexibility in the matching process. Then decide a task (explained in next chapter) and specify a delete limit. The delete limit will override the default severity-limit specified in xaps-core.properties for this particular message type. In short it means that if you want to retain some messages for a longer time than default (which is to delete a INFO-level message after 7 days from the Fusion DB), you can keep one type of INFO-messages longer. If delete limit is set to 0, default limits are used (from xaps-core.properties).

14.1 Syslog tasks

The task tells the Fusion Syslog server what kind of action to perform.

14.1.1 STORE

The STORE task simply stores the message in the database. This is default behavior for all messages, and is listed here for completeness sake.

14.1.2 DISCARD

The DISCARD task throws the message away. This is particularly useful when devices send a large amount of messages with high severity. In that case you cannot easily raise the log level on the client, because you would then filter out important messages as well.

14.1.3 DCT

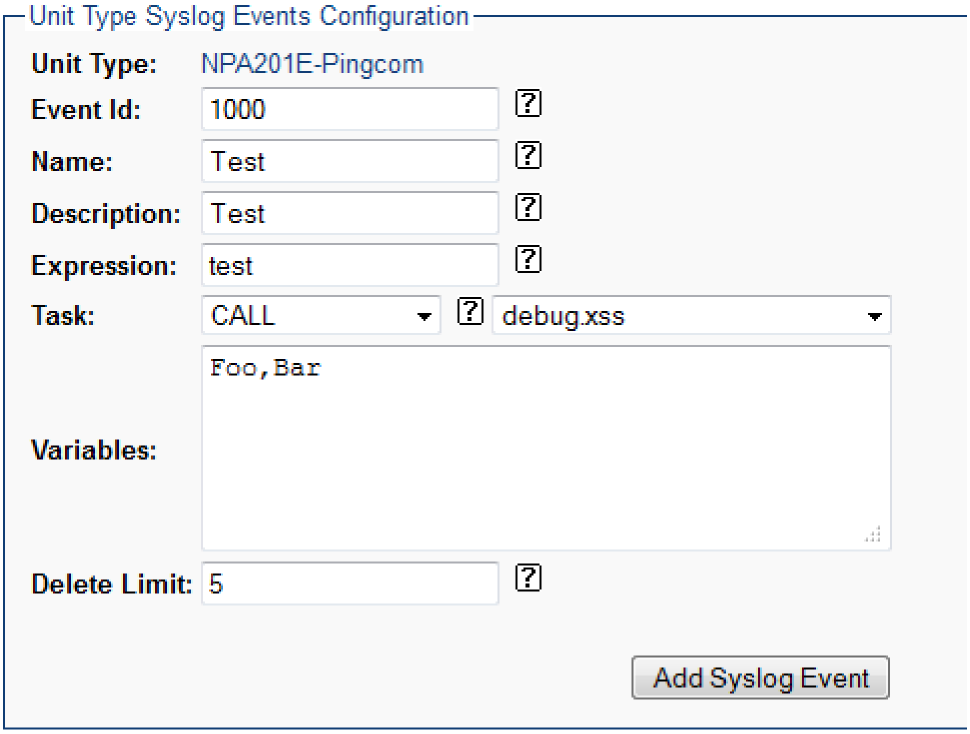
DCT is short for Duplicate Content Task. The task will compare every incoming syslog message with older messages, to search for duplicates. If the content of the message matches exactly, the message itself will not be written to the syslog database. However, a counter will be updated, so that in the end a message will be written to the database saying that X duplicates where received. This task requires an extra argument, to tell the system how "far back" one should look for duplicates. A recommendation is 30 (minutes), so that the maximum number of a message that repeats a lot is once every 30 minute. By increasing the time you will need a larger buffer of "old messages" to compare with. This is controlled in the xaps-syslog.properties, to avoid too great memory consumption.

14.1.4 DUCT

DUCT is short for Duplicate Unit Content Task. The task is similar to DCT, but the duplicate matching requires that both Unit-id and content of message must be the same.

14.1.5 CALL

The call task will execute a Fusion Shell script found in the Fusion DB. Upload a file of type SCRIPT into the Files section, and then you can select the script from the drop-down. You can also pass arguments into the script. In the screen shot below, two arguments are passed, and they are retrieved using ${_1} and ${_2} in the Shell script.



Unit Type Syslog Events Configuration

Unit Type:	NPA201E-Pingcom
Event Id:	1000
Name:	Test
Description:	Test
Expression:	test
Task:	CALL ▾ debug.xss ▾
Variables:	Foo,Bar
Delete Limit:	5

You can read more about the possibilities in Fusion Shell User Manual, but one idea is to change settings on Unit configuration (or Profile for that matter) based on the content of a syslog message. Image an ERROR message appear from one device. You may want to change the log level on this device to "DEBUG". And you may even want to kick the device, to get an immediate provisioning. All this is possible (and much more) using shell. It is furthermore important to understand that every time the script is invoked, it is invoked in the context of that particular Unit that emitted the syslog message. This is important to be able to change the settings of the correct Unit.

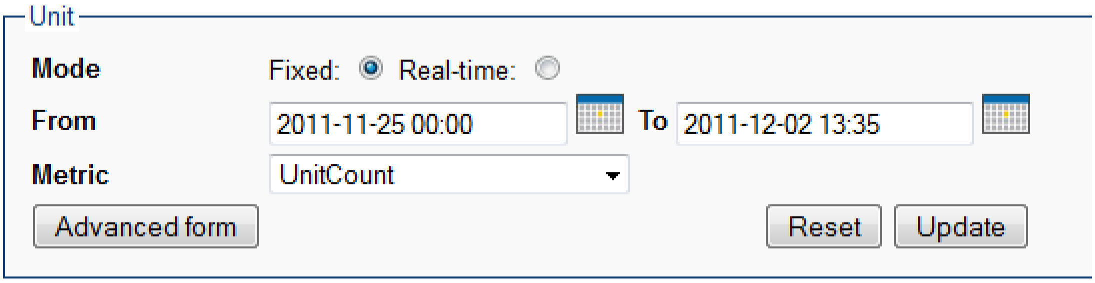
14.1.6 GROUPSYNC

A GROUPSYNC task will copy the time rolling parameter value of the group (which you choose in the drop down) into the appropriate Unit configuration (which is the Unit that emitted the syslog message). The concept is to mark units with a timestamp every time a certain message appear. Then (will be discussed later) the reports will count the size of these time rolling groups and thus count the occurrence of the syslog message.

15 Reports

Fusion provides a set of reports, as well as the ability to make your own custom reports. These reports provides a way to get an excellent overview over many things that goes on in Fusion as well as the devices.

All reports offer the same interface:



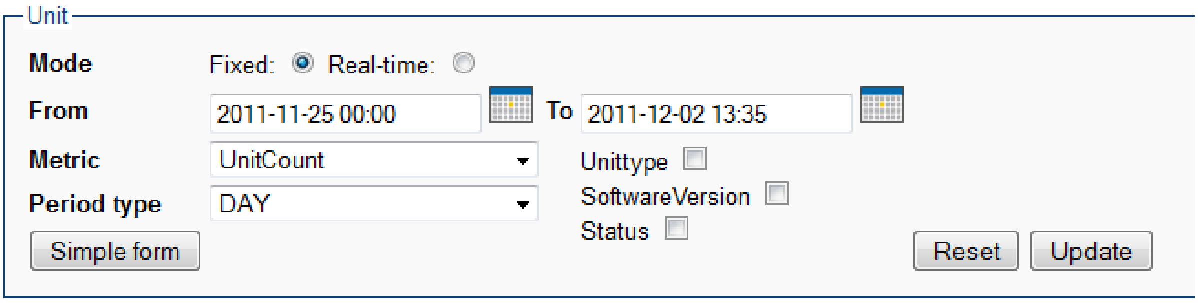
Unit

Mode Fixed: ● Real-time: ○
From 2011-11-25 00:00 To 2011-12-02 13:35
Metric UnitCount

At the top you can choose to access a report in a "Fixed" time. The From and To are set below. If you choose "Real-time", the report will update every 5 seconds and constantly show the last 5 minutes. This is not meaningful unless the report data changes very often, so this feature is only used for reports based on syslog data.

The Metric drop-down contains all metrics available for the report. For some report (like Unit report), only one single metric is available.

You may choose the Advanced Form too see some additional features:



Unit

Mode Fixed: ● Real-time: ○
From 2011-11-25 00:00 To 2011-12-02 13:35
Metric UnitCount
Period type DAY
Unittype □
SoftwareVersion □
Status □

In advanced form you can choose the Period Type. This is usually set to "DAY", but can be changed to "MONTH" or "HOUR" (in some cases even MINUTE or SECOND). By changing the period type, the data is aggregated on the new period. Thus, if you want to study a long time period (several months), it is better and faster to change the period type to MONTH (than HOUR) in case you're interested in the long term trends. However, if the extremes are of most interest, HOURly period may be the best.

The check-boxes at the right allows you to focus on one or several factors of special interest. By checking Unittype, you will get to see the chart of the metric for each Unit Type. If you also check SoftwareVersion, you get to see the chart of the metric for every combination of Unit Type and SoftwareVersion. This is a powerful way of analyzing important factors of a trend.

The last common feature of reports is the ability to click on the chart. By clicking on the chart "dots", you will zoom into a period type of higher granularity (ex: MONTH->DAY).

You will also zoom into that particular day or hour (depending upon which period type you came from). This is a quick way to identify the exact time for a change. You can also click on the legends at the right side of the chart, which will then mark the associated chart line.

15.1 Fusion Reports

The Fusion Reports focus on the concepts that are of most interest for the Fusion Server as such. Those are Unit, Group and Job reports.

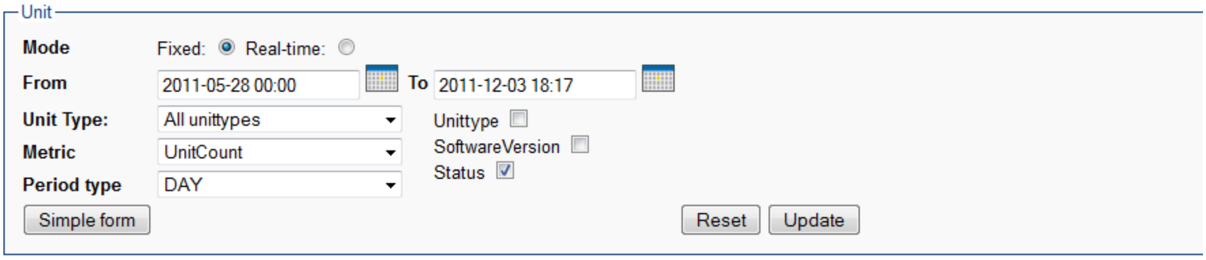
15.1.1 Unit Report

A unit report offers the Unit-count. The use-cases for this report is to answer (among others) the following question:

- how many units are deployed?
- how many units are found in each profile?
- what is the growth-trend over the last 6 months?
- what software-versions are deployed?
- how many devices are not in contact with the provisioning server?

The Profile check-box will not be shown unless you have chosen one particular Unit Type in the Context Bar. The status check-box will cause the report to show provisioning-connect-status.

Example:



Unit

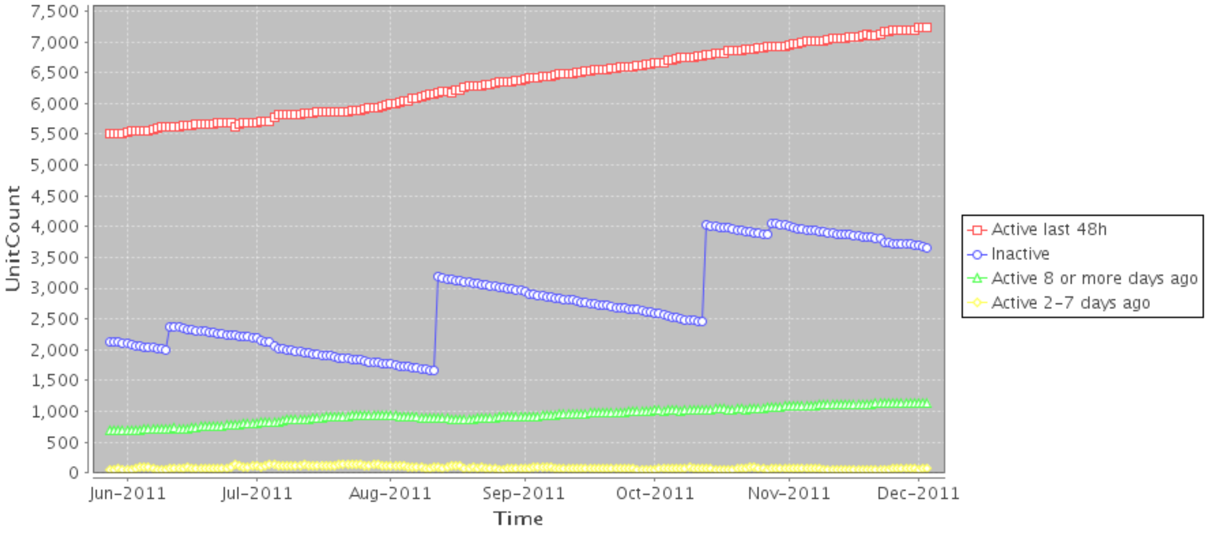
Mode Fixed: ● Real-time: ○

From 2011-05-28 00:00 **To** 2011-12-03 18:17

Unit Type: All unittypes — Unittype □

Metric UnitCount — SoftwareVersion □

Period type DAY — Status ☑

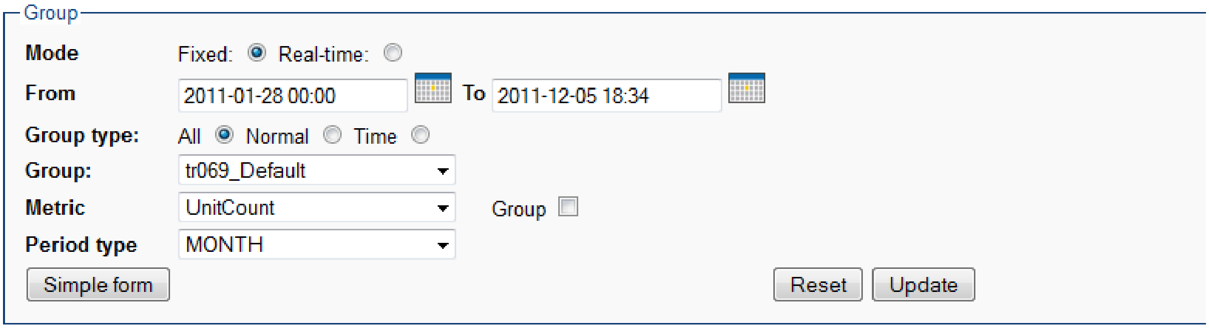


The example shows how the number of "Active last 48h" devices increase steadily over time. Furthermore, the pool of registered, but Inactive (not yet deployed, or never connected by the customer) increase suddenly and then drops off steadily.

In this example the most worrying trend is the rising number of "Active 8 or more days ago" devices increases. This could mean an increasing number of customers which have been active, but where the device for some reason no longer connects to Fusion. This could indicate technical problems or a customer which no longer uses the equipment. To investigate further one should look into Fusion Shell to make lists of all those devices which has a LastConnectTms which is too old.

15.1.2 Group Report

A group report offers one metric: The unit count. By creating groups that varies in size according to some changes on the system, these reports can be quite interesting. As previously discussed this could be time rolling groups, detecting syslog message occurrences, or normal groups which may detect the occurrence of a certain set of parameters (like software version). Example:



Group

Mode Fixed: ● Real-time: ○

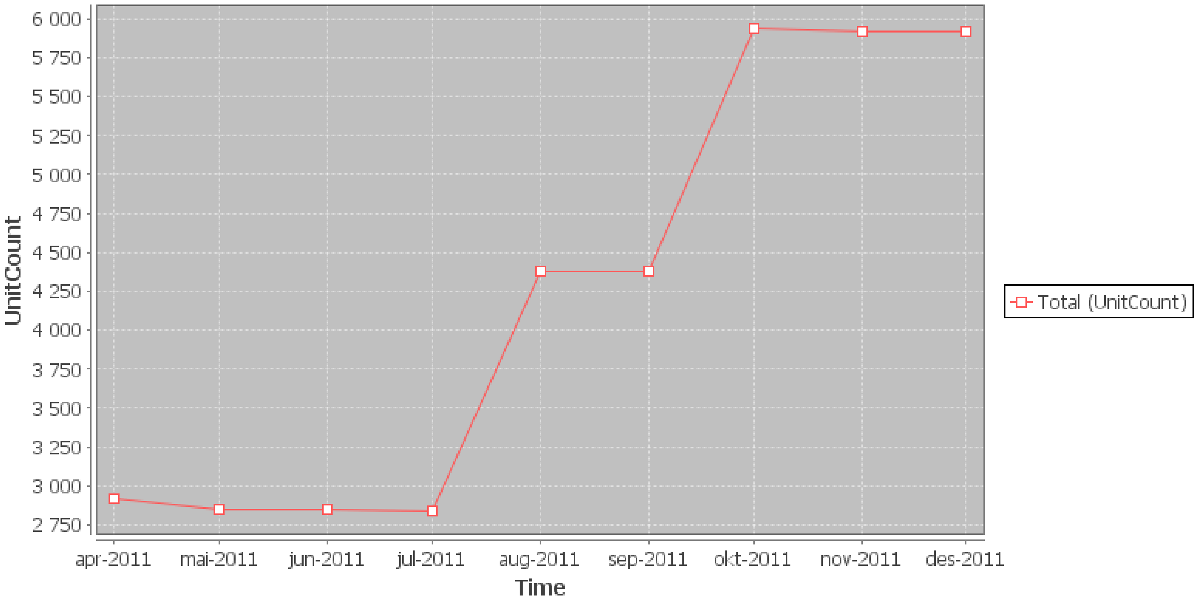
From 2011-01-28 00:00 **To** 2011-12-05 18:34

Group type: All ● Normal ○ Time ○

Group: tr069_Default

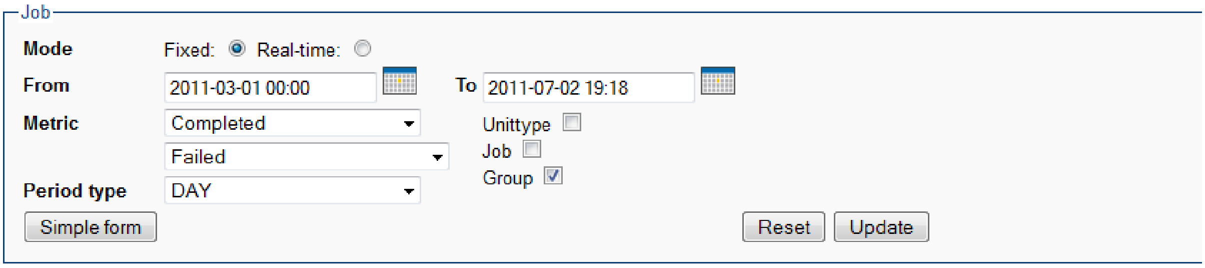
Metric UnitCount Group ☐

Period type MONTH



15.1.3 Job Report

Job report offers metrics for completed (ok) jobs, and for various states (confirmed failed, unconfirmed failed, failed, and for group size. Since more than one metric is available, you may choose two metrics to be shown in one chart. Example:



Job

Mode Fixed: ● Real-time: ○

From 2011-03-01 00:00 **To** 2011-07-02 19:18

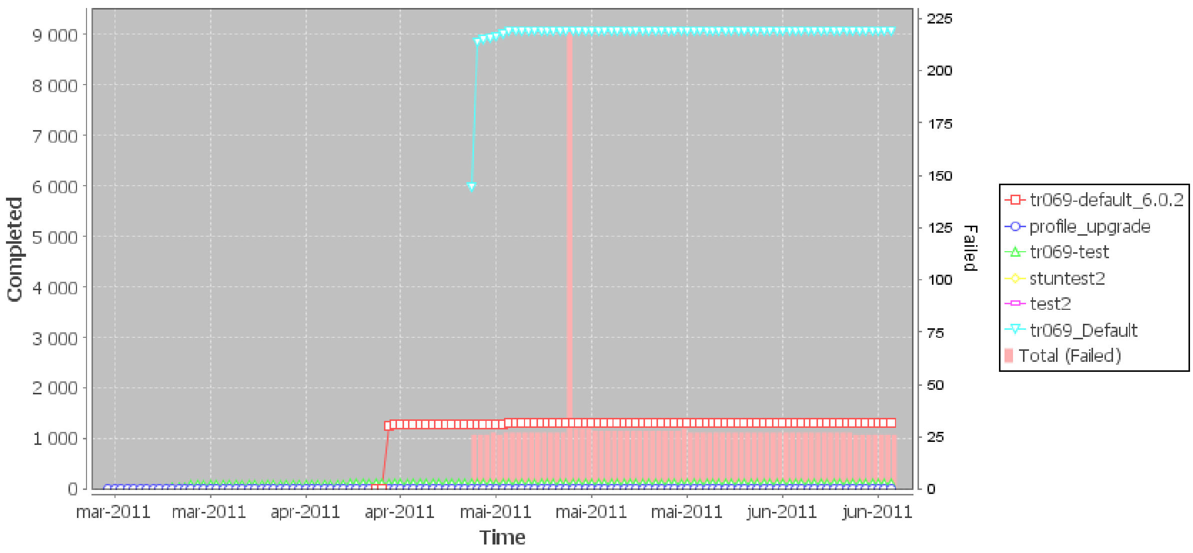
Metric Completed / Failed

Unittype □

Job □

Group ☑

Period type DAY



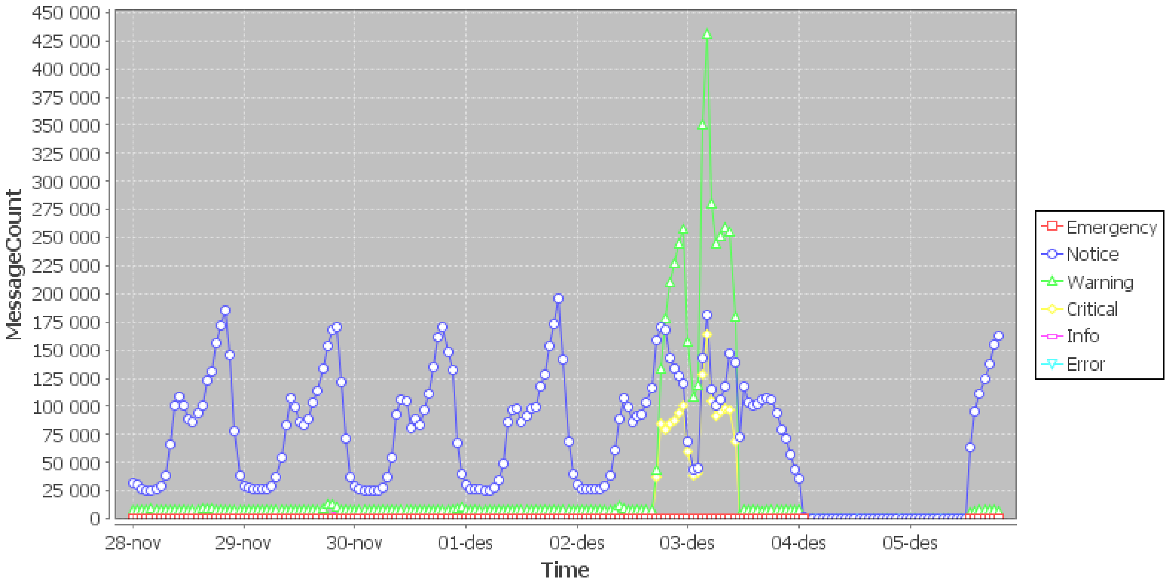
The example above shows the number of completed jobs for each group in the current Unit Type/Profile. The Total-legend refers to the total number of "Failed" jobs within the Unit Type/Profile chosen.

15.2 Syslog reports

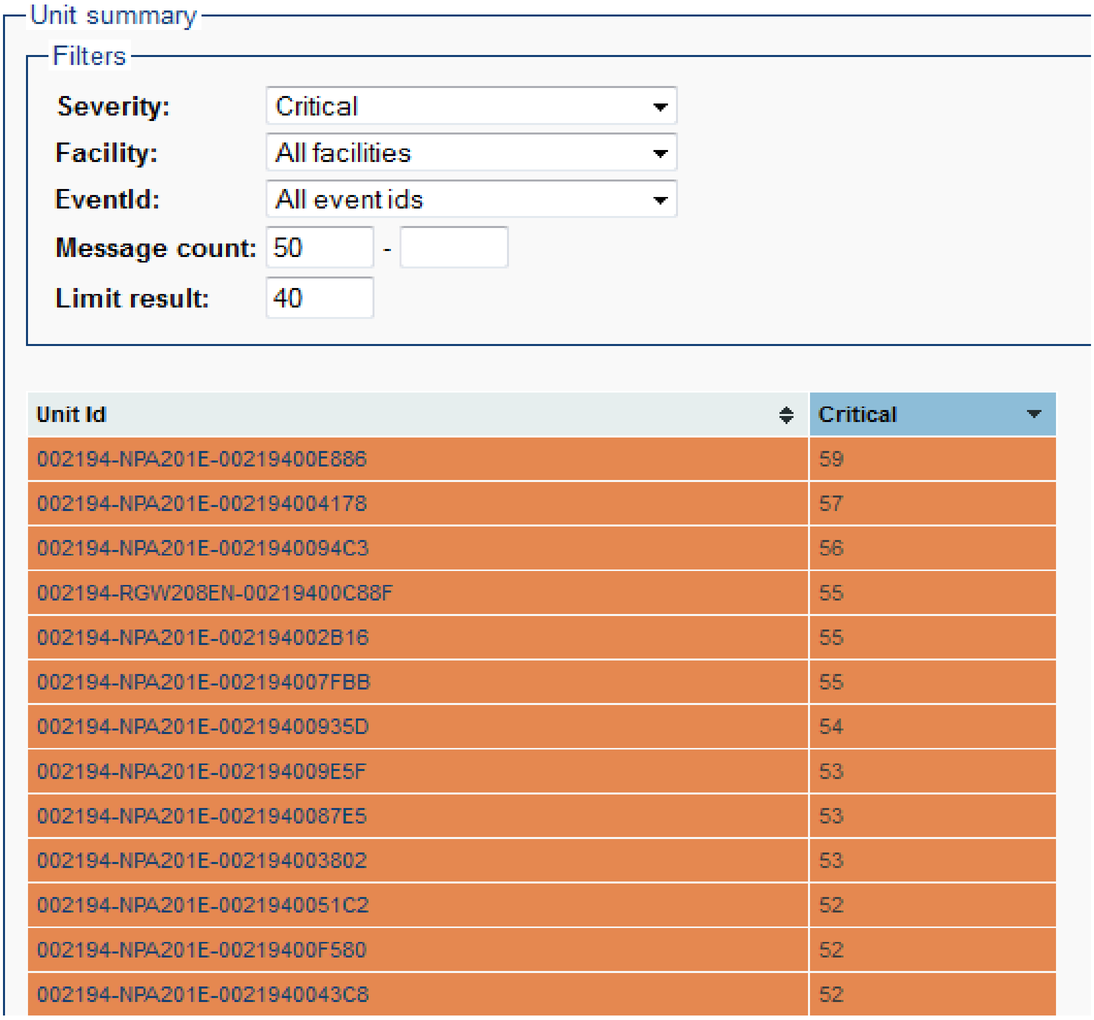
Syslog reports are built upon the syslog data gathered by the Fusion Syslog server. One goal with syslog is to provide a framework for logging from devices and to show how easily Fusion can utilize the data in terms of reports. Another aspect of syslog is that the data gathered unit-by-unit can be inspected, zooming in from "all-units-level" down to the "single-unit-level". This makes it possible to identify the causes of the various anomalies that are observed in the reports.

15.2.1 Syslog report

The most basic syslog report is simply a report that counts the number of messages, severities and facilities from the syslog. This is useful to give you a hint of the state of the system and the pool of devices. Since it is possible to log directly from each module in Fusion DB, you can spot error messages coming from all kinds of the system in one place. Consider a situation like this:



In this case we might be interested in the "Critical" syslog messages. To inspect further, simply click on a yellow point in the chart and observe a page containing all units with critical messages within the given hour.


Unit summary

Filters

Severity:	Critical		
Facility:	All facilities		
EventId:	All event ids		
Message count:	50	-	
Limit result:	40		

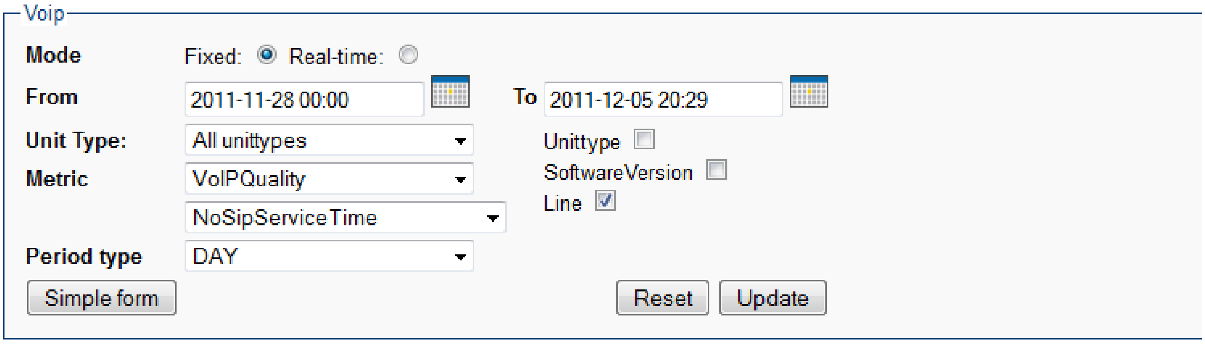
Unit Id	Critical
002194-NPA201E-00219400E886	59
002194-NPA201E-002194004178	57
002194-NPA201E-0021940094C3	56
002194-RGW208EN-00219400C88F	55
002194-NPA201E-002194002B16	55
002194-NPA201E-002194007FBB	55
002194-NPA201E-00219400935D	54
002194-NPA201E-002194009E5F	53
002194-NPA201E-0021940087E5	53
002194-NPA201E-002194003802	53
002194-NPA201E-0021940051C2	52
002194-NPA201E-00219400F580	52
002194-NPA201E-0021940043C8	52

At this point you can sort the list of units on the count, and you can adjust the filter settings to inspect only those of interest. Finally you may click on the unit-id you want to inspect and examine the individual syslog messages further, as well as other settings on the Unit.

Keep in mind, that this last level of inspection is not possible when the messages are deleted from the syslog table. This is for the most part controlled in xaps-core.properties, but could be overruled by a Syslog Event.

15.2.2 VoIP report

A VoIP report is designed to give you full overview of the VoIP service. The report offers several metrics, like VoIPQuality, MOS (Mean Opinion Score), SIP-Server-Downtime, etc. Currently only devices from Ping Communication support this kind of report, but the format of the syslog message is freely available and any capable VoIP-engine can support this kind of message if requested by a customer. Example:



Voip

Mode Fixed: ● Real-time: ○

From 2011-11-28 00:00 **To** 2011-12-05 20:29

Unit Type: All unittypes

Metric VoIPQuality

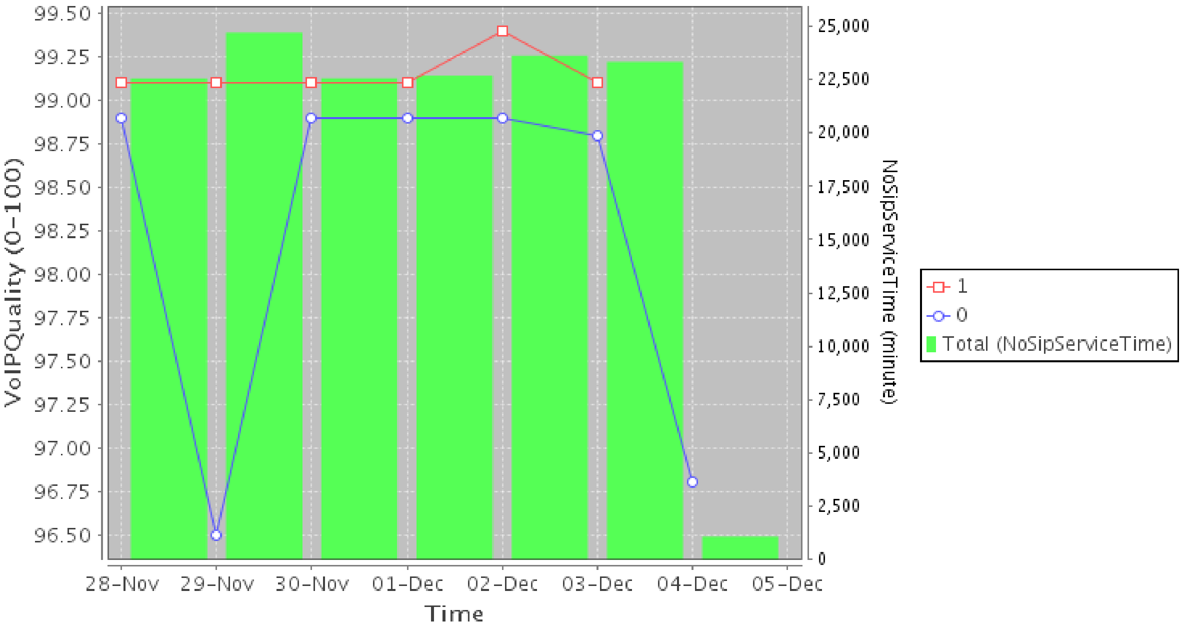
NoSipServiceTime

Period type DAY

Unittype □

SoftwareVersion □

Line ☑

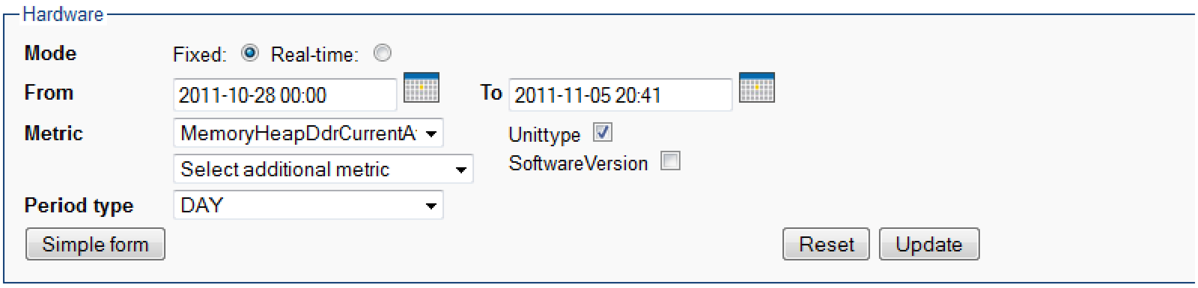


The chart shows a sharp decrease in VoIPQuality while at the same time the "NoSipServiceTime" increases. This shows that at least part of the reason for the drop in quality is the downtime on the SIP-server. Also note that VoIPQuality varies for Line 0 and Line 1. Always look close at the y-axis, which always adjust to max and min values in the chart. Therefore, a radical change on the chart may not be a lot in absolute values.

As for other syslog reports, you may zoom in to identify exact time and Units responsible for reporting this situation.

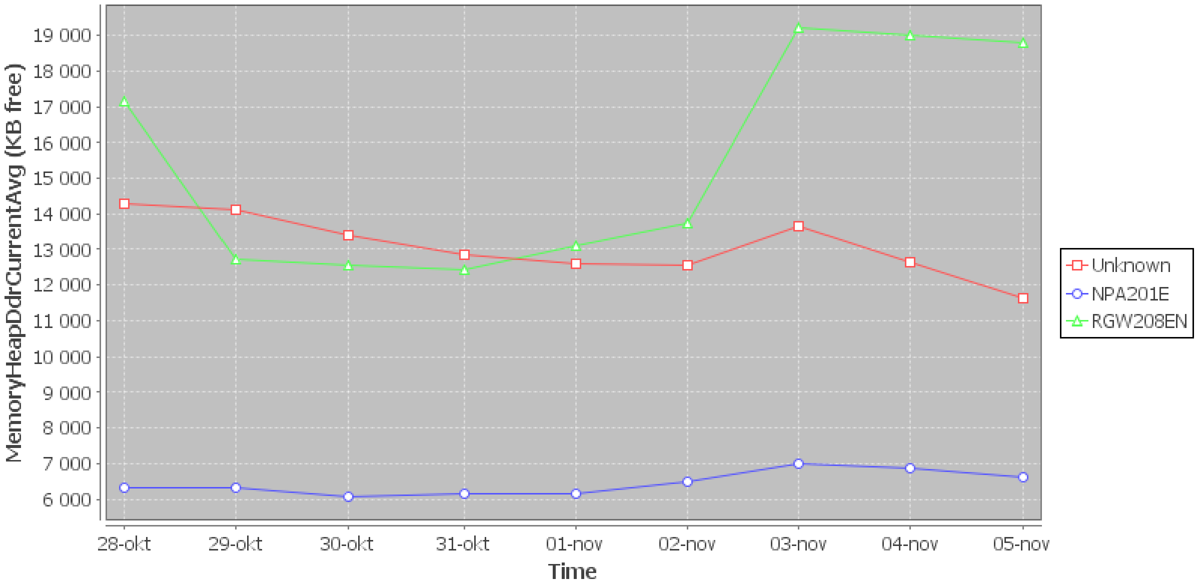
15.2.3 Hardware Report

The hardware report also provides a lot of metrics, but focuses mainly on boots and memory situation. Both of these issues are very important for the operator, and will provide him with a good insight in how the stability of the devices are. Example:



Hardware

Mode	Fixed: ● Real-time: ○		
From	2011-10-28 00:00	To	2011-11-05 20:41
Metric	MemoryHeapDdrCurrentA	Unittype	☑
	Select additional metric	SoftwareVersion	□
Period type	DAY		

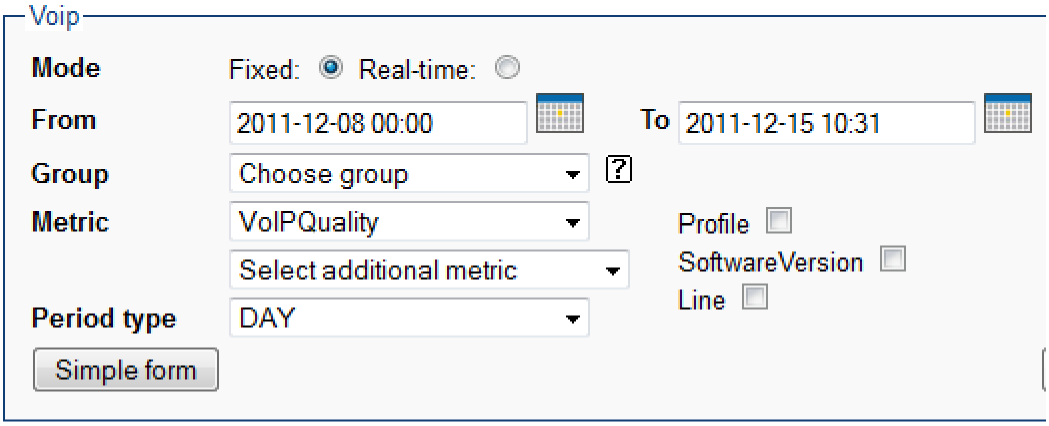


The chart shows a falling trend in memory consumption, specifically the memory consumption of DDR-ram. The report is currently only supported by Ping Communication products, but other device vendors are free to implement the simple syslog messages necessary to produce these reports.

15.2.4 Dynamic selection of units

All reports discussed so far has been based on one or all Unit Types, or one or all Profiles. This is not entirely satisfactory, since you may want to study for example VoIP quality for a certain set of Units. All reports based on syslog data can overcome this limitation and again the Group will come in handy: Make a Group selection for those Units of particular interest (they must have a common value[1]; e.g., all IP address starts with "202.101", or a combination of common values). Make sure to select a Unit Type and choose Advanced. Then you should see something like this:

[1] A common value may also be achieved by making a new Unit Type Parameter, and assigning a common value to all those Units of special interest.



Voip

Mode Fixed: ● Real-time: ○

From 2011-12-08 00:00 To 2011-12-15 10:31

Group Choose group

Metric VoIPQuality

Select additional metric

Profile □

SoftwareVersion □

Line □

Period type DAY

The Group drop-down will show up and make it possible to choose groups within the particular Unit Type or Profile that has been chosen. However, this kind of report generation is dynamic, meaning that the report data has not been preprocessed and ready. Thus it will take more time to generate (reading the data directly from the syslog database and aggregating the metrics), so be careful about the timespan you choose. Also, the syslog data are deleted (according to xaps-core.properties and syslog event deletion rules) so if you go to far back, you may not find any data.

15.3 TR reports

The final category of reports in Fusion is TR-reports. These reports build upon data collected through TR-069 parameters and through the usage of the TR-069 server. The setup of these reports are described in Fusion Shell User Manual. The collection of the data is always transmitted to the syslog table, in a compressed format, so it will still be possible to trace the various changes in the chart back to the individual Units. Some limitations of the reports must be mentioned. First and foremost is the performance limitation. One should not try to run these data collector jobs to often (too small repeat interval) and not run the job on too large a group. The simple reason, is that if you do it will in effect be the same as doing regular provisioning on a pool of devices that is 10 or 100 times bigger that your pool today. So the advice is to be a little cautious and increase the groups that participate in this kind of reporting slowly.

Furthermore, the devices must support a number of TR-parameters (Fusion Shell will check this upon setup), parameters which may not be too common.

The reports that are offered are VoIP, Hardware and Gateway. This is an alternative to the better and more specialized syslog reports.