User Guide to the Snare Agent Management Console in Snare Server v7.0

Table of Contents

1. Overview

ⓘ **About this User Guide**

This user guide describes how to use the Agent Management Console within the Snare Server product. This guide targets the console that was launched in v7.0.x of the Snare Server. If you are using an earlier, or later, version of the server, please refer to the User Guide for that version instead as there may be significant changes between versions.

It is designed to be a starting point for users who already have a working Snare Server v7.0.x installation, and are familiar with the basic navigation concepts. For help installing the server, please refer to the Snare Server v7.0 Installation Guide. Likewise, if you are running an older version (v6, v5 or v4), then please update your Snare Server version first.

This guide also assumes that you have at least one working Snare Agent within your environment. Please refer to the associated Agent user guides if you need any help installing your Agents. Please also refer to the Compatibility Chart to ensure that the Agents you are using are compatible with the console.

1.1. What is the Agent Management Console (AMC)?

The AMC is a tool within the Snare Server that enables remote management of Snare Agents through the Snare Server interface.

The AMC enables administrators to set up automatic audits of the configuration of Agents within their fleet. The administrators specify a *Master Configuration,* which represents the required configuration of the fleet Agents. This Master Configuration is then compared to the actual configuration of each of the Agents within their fleet. Any discrepancies that are found are listed, and alerts sent out as required. Any Agents that were uncontactable during the process are also identified. The results of these configuration audits provide information to the administrators that can be used to identify if the configurations of any Agents have been unexpectedly modified.

The AMC also provides the ability to push the specified *Master Configuration* out to each of the Agents under management to enable fleet-wide configuration changes from a centralised location. This also ensures that any unauthorised configuration changes on the Agents are reverted automatically.

Snare Agents that are reporting directly to the Snare Server are automatically detected by the AMC. For other situations where there are Agents that are not reporting directly to the Snare Server, a list of custom Agents can be manually added into the AMC.

1.2. What the Console CAN do

The Agent Management Console allows you to create as many Management Objectives as is required in your environment. These objectives allow you to:

- Manage **any** compatible Snare Agent, even if it is not directly reporting to the Snare Server.
    - Snare Agents reporting to the Snare Server (via ports 6161 or 514) will be automatically identified and treated as a *reporting Agent*.
    - Snare Agents not reporting to the Snare Server can be manually added within the Management Objective configuration, as a *non-reporting Agent*. After manually specifying these Agents, the management functionality available is exactly the same as a *reporting Agent*.
- Specify the specific type of Agent to be managed (to ensure configurations aren't corrupted by passing the wrong configuration).
- Pull the current configuration from any of the compatible Snare Agents within your environment.
    - Either by filtering Agents that report event logs to the Snare Server by hostname and/or version,
    - Or by specifying non-reporting Agents manually by IP (or IP range).
- Pull current configuration from a specific Master Agent to compare against the managed Agent configurations.
- Optionally push the master configuration out to each of the managed Agents that support push, to sync configurations to a single configuration.
- Set a specific schedule to run the configuration check/sync process.

- Send email alerts when Agents are uncontactable and/or have a different configuration.

1.3. What the Console CANNOT do

- The Agent Management Console currently only manages Agent Configurations for **compatible Enterprise Agents**.
- It does not provide the ability to install and/or upgrade the Agent software.
- It will only work on Agents that have the Remote Management function enabled, without this, the Console cannot communicate with the Agent.
- All communication is initiated by the Server, so firewall rules must be in place to allow the Server to connect to each Agent.
- The Console cannot monitor/wait for an Agent to come online - if it is not online when the check/sync is triggered, it will be considered uncontactable.

1.4. Snare Agent Compatibility

Agent	Version(s)	Config Pull	Config Push
Enterprise - Snare Agent for Windows	v4.x	✓	✓
Enterprise - Snare Agent for Windows	v4.0.2.x	✓	✗
Enterprise - Snare Agent for Windows	v4.0.0.0, v4.0.1.x	✓	✓
Enterprise - Snare Agent for Linux	v1, v2.1, v3, v4	✓	✗
Enterprise - Snare Agent for Solaris	v3.0.x - v3.2.x	✓	✗
Enterprise - Snare Epilog	*any*	✗	✗
Enterprise - Snare for MSSQL	*any*	✗	✗
Open Source - Snare Agent/Epilog	*any*	✗	✗
Snare Browser Agents	*any*	✗	✗

Notes:

- *Compatibility table refers to Snare Server v7.0.x only.*
- "*Config Pull*" means Agent Configuration can be retrieved from the Agent by the Server.
- "*Config Push*" means Agent Configuration can be updated by the Server on the Agent.

2. Getting Started

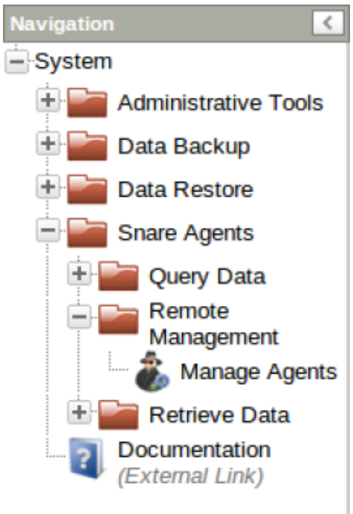
2.1. Requirements

In order to start using the Agent Management Console you need the following:

- Installed and working Snare Server v7.0.0, or newer.
- Installed and working Snare Agents, which are compatible with the console as listed in 1.4 above.
- Firewall rules that allow the Snare Server to initiate a connection with the Snare Agent on the specified Agent Remote Management port (usually 6161).
- Remote Management enabled on the Snare Agent(s) with a known port and password.
- Remote Management on the Snare Agent(s) allowing connections from the Snare Server IP address.

2.2. Accessing the Console

The Agent Management Console is located in the *'System'* section (button top right), and found under '*Snare Agents*' > '*Remote Management*' in the left side navigation menu.

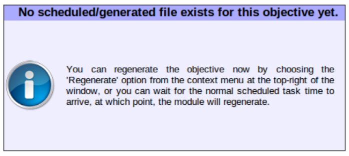


By default a single objective is created within this section: '*Manage Agents*'.

It is possible to create as many objectives as required, following the standard Snare Server method of cloning an existing objective. Simply *right-click* on the existing *Manage Agents* objective and select *Clone* from the menu.

Likewise, these objectives can be easily *renamed* and *deleted* from the *right-click* menu as well. It is also possible to change the icon of the objective, through the final option in the *right-click* menu, in order to make it stand out from the others.

By default, each new objective starts off with a friendly message to inform you that it has not been configured yet. To configure the objective, simply click on the *Configure* icon in the top tool bar. Once your objective has been successfully configured, you can click the *Regenerate* button to trigger the configuration check and sync.



No scheduled/generated file exists for this objective yet.

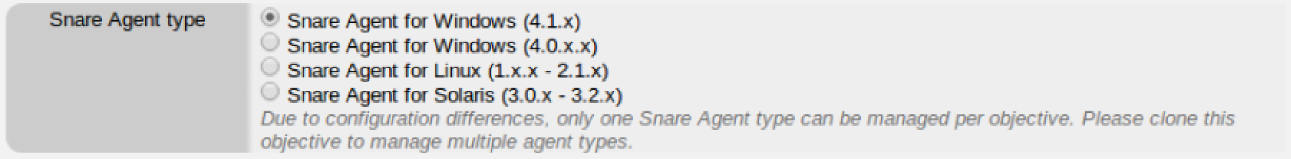
You can regenerate the objective now by choosing the 'Regenerate' option from the context menu at the top-right of the window, or you can wait for the normal scheduled task time to arrive, at which point, the module will regenerate.

Each objective can be scheduled, like any other Snare Server Objective. Simply click the *Schedule* button in the toolbar and the schedule options will appear. Likewise, you can also configure the *Access Control* and download the objective report as an *Attachment* through their own buttons too.

3. Configuration

The Agent Management Console Objective Configuration is accessible by clicking on the *Configure* icon in the top toolbar. It will bring up a dialog with a number of different selections, each of which are covered below.

3.1. Snare Agent Type



Snare Agent type

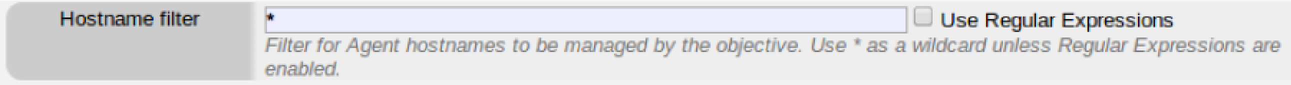
● Snare Agent for Windows (4.1.x)
○ Snare Agent for Windows (4.0.x.x)
○ Snare Agent for Linux (1.x.x - 2.1.x)
○ Snare Agent for Solaris (3.0.x - 3.2.x)

Due to configuration differences, only one Snare Agent type can be managed per objective. Please clone this objective to manage multiple agent types.

Due to the differences between the functionality and capability of each of the different Snare Agent types, it is a requirement to specify the type of Agent to be managed via the Console. Any Agent that is contacted, but of a different type, will be marked as such and ignored by the configuration checking.

To manage multiple types of Snare Agents, please clone an existing objective and change the type on the cloned objective(s) to cover the different versions as required.

3.2. Hostname filter



Hostname filter: *

□ Use Regular Expressions

*Filter for Agent hostnames to be managed by the objective. Use * as a wildcard unless Regular Expressions are enabled.*

When dealing with reporting Agents (i.e. Agents that log events directly to the Snare Server), it is possible to filter Agents by hostname so only a specific subset are managed by the console. The filter can either be applied using a standard wildcard * character, or using Regular Expressions for more complex filters.

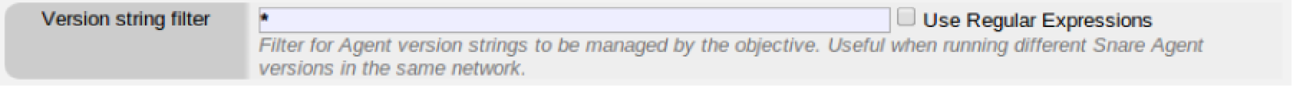
This option is quite useful when you have a large fleet of different Agents all reporting to the Server. As long as the host names on each of the Agents are correctly set up, you can easily filter out, for example, the workstations from the servers without needing to manually specify each one as it is provisioned.

Examples:

Hostname Requirements	**Examples**	**Wildcard Filter**	**Regular Expression**
All hosts within the domain dni.gov.au.	alpha.dni.gov.au beta.dni.gov.au	*.dni.gov.au	(.*)\.dni\.gov\.au
All hosts starting with win, and ending in c01.	win01-02c01 win02-02c01 win03-10c01	win*c01	win(.*)c01
Hosts starting with ws, and ending with either a 0, 1, or 2.	ws-17hm42 ws-abcw20 ws-87sde1	*Not possible with a standard wildcard.*	ws(.*[012])

Note: The hostname filter is bypassed when an agent is specified as a *Non-reporting Agent*. When working with non-reporting Agents only, you can specify a long string of random characters in this field to prevent any reporting agents from being managed by mistake.

3.3. Version string filter



Version string filter

*

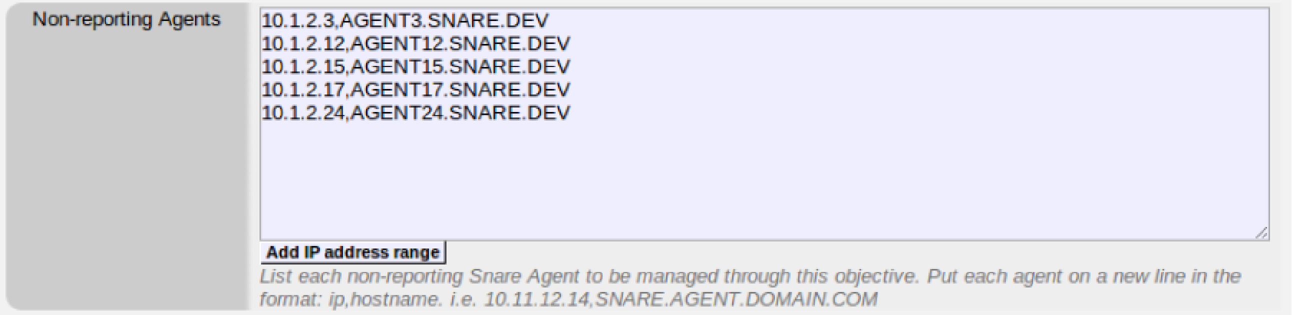
☐ Use Regular Expressions

Filter for Agent version strings to be managed by the objective. Useful when running different Snare Agent versions in the same network.

Similar concept to the *Hostname filter*. The version string applies to the Agent version number reported by the agent for the reporting Agents (again, this is ignored when dealing with a non-reporting Agent). It supports the same wildcard or regular expression filtering as the hostname filter.

This option is only useful when you have different versions of the Agent installed for different purposes. It can normally be left as a wildcard, since the Snare Agent Type selection above handles the major version difference selection.

3.4. Non-Reporting Agents



Non-reporting Agents

```
10.1.2.3,AGENT3.SNARE.DEV
10.1.2.12,AGENT12.SNARE.DEV
10.1.2.15,AGENT15.SNARE.DEV
10.1.2.17,AGENT17.SNARE.DEV
10.1.2.24,AGENT24.SNARE.DEV
```

List each non-reporting Snare Agent to be managed through this objective. Put each agent on a new line in the format: ip,hostname. i.e. 10.11.12.14,SNARE.AGENT.DOMAIN.COM

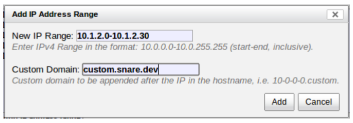
When you need to manage Agents that do not report to the Snare Server you are using for the Agent Management Console, you can specify them in the Non-Reporting Agents section. There are two ways to enter agents to be managed.

Either manually enter them into the box, one per line in the format:

```
[ipaddress],[hostname]
```

For example:

```
10.1.2.3,AGENT3.SNARE.DEV
10.1.2.12,AGENT12.SNARE.DEV
10.1.2.15,AGENT15.SNARE.DEV
10.1.2.17,AGENT17.SNARE.DEV
10.1.2.24,AGENT24.SNARE.DEV
```



Add IP Address Range

New IP Range: 10.1.2.0-10.1.2.30

Enter IPv4 Range in the format: 10.0.0.0-10.0.255.255 (start-end, inclusive).

Custom Domain: custom.snare.dev

Custom domain to be appended after the IP in the hostname, i.e. 10-0-0-0.custom.

Or you can add an entire IP address range, using the button *Add IP address range* under the box. This will present you with a dialog to enter in the IP range and the custom domain to be appended onto the end of the domain.

For example, you enter the IP range: 10.1.2.0-10.1.2.10

With the custom domain: custom.snare.dev

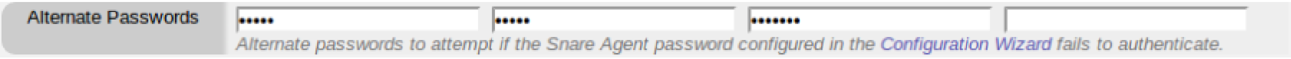
Then your non-reporting Agents box would be automatically filled with these Agents:

```
10.1.2.0,10-1-2-0.custom.snare.dev
10.1.2.1,10-1-2-1.custom.snare.dev
10.1.2.2,10-1-2-2.custom.snare.dev
10.1.2.3,10-1-2-3.custom.snare.dev
10.1.2.4,10-1-2-4.custom.snare.dev
10.1.2.5,10-1-2-5.custom.snare.dev
10.1.2.6,10-1-2-6.custom.snare.dev
10.1.2.7,10-1-2-7.custom.snare.dev
10.1.2.8,10-1-2-8.custom.snare.dev
10.1.2.9,10-1-2-9.custom.snare.dev
10.1.2.10,10-1-2-10.custom.snare.dev
```

Using a combination of these two input methods, you should have no trouble easily adding in all of the non-reporting Agents that you wish to manage through the console.
Notes:

- Non-Reporting Agents bypass the specified *hostname* and *version string* filters, but not the *Snare Agent Type* selection. This means every Agent listed in the non-reporting Agents box will be managed, as long as it is the right type.
- To tell the console to ignore all reporting Agents and only manage non-reporting Agents, simply set the *Hostname filter* to a pile of random characters that does not exist in a hostname, i.e. '*thiswillnotexistinahostnamesoonlynonreportingagentswillbefound*'.
- It is not possible to set only a hostname with no IP address for a non-reporting Agent.

3.5. Alternate Password



Alternate Passwords ••••• ••••• •••••••

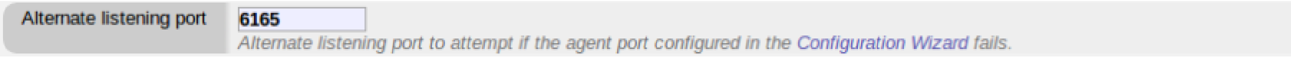
Alternate passwords to attempt if the Snare Agent password configured in the Configuration Wizard fails to authenticate.

The Console needs to authenticate each Agent with a valid password, as specified on the Agent. The master password is specified in the *Snare Configuration Wizard*, however if that password fails to authenticate, then these options provide a backup. Each of the alternate passwords are tried in turn until a successful authentication attempt is found. This allows the objective to manage a group of Agents with up to 5 unique passwords.

This option is useful if you have assigned different Agent Remote Management passwords for different groups of Agents, so you can manage them all from a single point, or have different password(s) configured in each objective. It is also quite handy when you have a password rotation plan, since you can enter in the old passwords into the alternate boxes to ensure that Agents that haven't been updated yet can still be communicated with.

Note: When configuration push is enabled, the password assigned on the Master Agent will be pushed out to all the managed Agents, causing them to all have the same password.

3.6. Alternate listening port



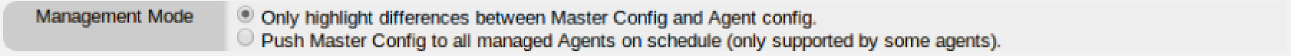
Alternate listening port 6165

Alternate listening port to attempt if the agent port configured in the Configuration Wizard fails.

Similar to the Alternate Password option, this option allows you to specify an alternate port to connect to the Snare Agent on. It will first attempt to use the port found in the Snare Configuration Wizard, and if that fails, it will use this one instead.

The only reason this option will need to be used is if you have changed the default port of the Snare Agent from 6161 for whatever reason.

3.7. Management Mode


Management Mode
● Only highlight differences between Master Config and Agent config.
○ Push Master Config to all managed Agents on schedule (only supported by some agents).

The Management Mode option allows you to chose between two options:

3.7.1. Only highlight differences between Master Config and Agent Config.

This option connects to each managed Agent, retrieves the current configuration, and then compares it with the master config only. It does not push back configuration changes to the Agents.

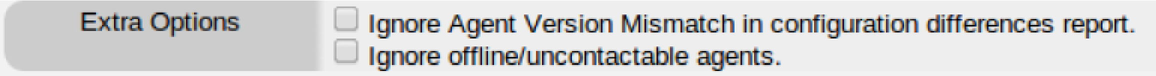
This is the default Pull-only option, and is the one to use when you only wish to regularly audit Agent configurations and be notified when anything changes. Note that some Agent versions will only work successfully with this option (see the compatibility chart in 1.3 above).

3.7.2. Push Master Config to all managed Agents on schedule (only supported by some agents).

This option connects to each managed Agent, retrieves the current configuration, compares it with the master config, and then pushes back any changes that it finds to compatible Agents.

This is the option to use when you want the Console to manage the Agent configuration for you. When a schedule is set up, it will automatically update the configuration on each Agent to ensure that it matches the master. If they cannot be synchronised, then the system will report the conflicts.

3.8. Extra Options


Extra Options
□ Ignore Agent Version Mismatch in configuration differences report.
□ Ignore offline/uncontactable agents.

3.8.1. Ignore Agent Version Mismatch in configuration differences report.

When this option is not enabled the Agent configuration checking will compare the Agent version with the master config Agent version. If they are found to differ, then it will list it as a configuration mismatch. This is useful when upgrading the fleet with new Agent versions to identify any that were missed, but if you intentionally use different versions of the Agent, then you can enable this option to ignore the differences.

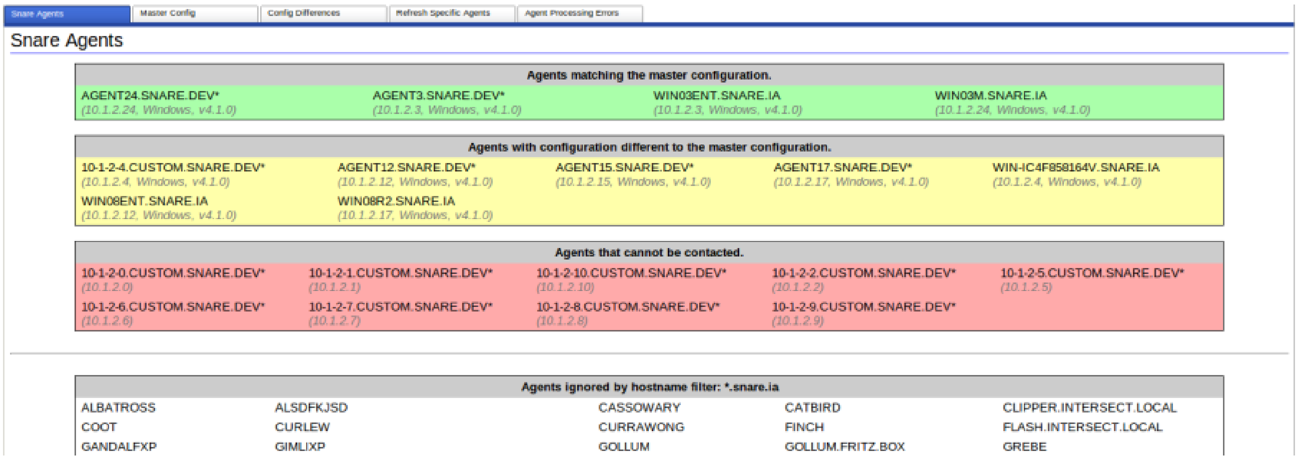
3.8.2. Ignore offline/uncontactable agents.

When an Agent cannot be contacted, it is highlighted as uncontactable, and it is listed as such in the report. Depending on your environment, you may want to disregard Agents that are offline (for example, when you add an entire IP range but only expect to find Agents on some of the IP addresses). If this is the case, then you can enable this option, and uncontactable Agents will no longer throw an alert (they will still be listed though).

4. Objective Output

Once the Console has been configured and regenerated, you will see the following output, and options.

4.1. Snare Agents



Snare Agents

Agents matching the master configuration.

AGENT24.SNARE.DEV* *(10.1.2.24, Windows, v4.1.0)*	AGENT3.SNARE.DEV* *(10.1.2.3, Windows, v4.1.0)*	WIN03ENT.SNARE.IA *(10.1.2.3, Windows, v4.1.0)*	WIN03M.SNARE.IA *(10.1.2.24, Windows, v4.1.0)*

Agents with configuration different to the master configuration.

10-1-2-4.CUSTOM.SNARE.DEV* *(10.1.2.4, Windows, v4.1.0)*	AGENT12.SNARE.DEV* *(10.1.2.12, Windows, v4.1.0)*	AGENT15.SNARE.DEV* *(10.1.2.15, Windows, v4.1.0)*	AGENT17.SNARE.DEV* *(10.1.2.17, Windows, v4.1.0)*	WIN-IC4F858164V.SNARE.IA *(10.1.2.4, Windows, v4.1.0)*
WIN08ENT.SNARE.IA *(10.1.2.12, Windows, v4.1.0)*	WIN08R2.SNARE.IA *(10.1.2.17, Windows, v4.1.0)*			

Agents that cannot be contacted.

10-1-2-0.CUSTOM.SNARE.DEV* *(10.1.2.0)*	10-1-2-1.CUSTOM.SNARE.DEV* *(10.1.2.1)*	10-1-2-10.CUSTOM.SNARE.DEV* *(10.1.2.10)*	10-1-2-2.CUSTOM.SNARE.DEV* *(10.1.2.2)*	10-1-2-5.CUSTOM.SNARE.DEV* *(10.1.2.5)*
10-1-2-6.CUSTOM.SNARE.DEV* *(10.1.2.6)*	10-1-2-7.CUSTOM.SNARE.DEV* *(10.1.2.7)*	10-1-2-8.CUSTOM.SNARE.DEV* *(10.1.2.8)*	10-1-2-9.CUSTOM.SNARE.DEV* *(10.1.2.9)*	

Agents ignored by hostname filter: *.snare.ia

ALBATROSS	ALSDFKJSD	CASSOWARY	CATBIRD	CLIPPER.INTERSECT.LOCAL
COOT	CURLEW	CURRAWONG	FINCH	FLASH.INTERSECT.LOCAL
GANDALFXP	GIMLIXP	GOLLUM	GOLLUM.FRITZ.BOX	GREBE

The default tab to be displayed provides a summary of the managed Agents, grouped by status. Each agent is listed by its *hostname* with its current *IP Address*, *Operating System*, and *Agent Version* listed in grey. Agents marked with a * are non-reporting Agents.

The possible status groups are:

4.1.1. Agents matching the master configuration.

These Agents were online and their config perfectly matched the Master Configuration.

4.1.2. Agents with configuration different to the master configuration.

These Agents were online, but their config was found to be different to the Master Configuration.

4.1.3. Agents that cannot be contacted.

These Agents were either offline, configured with an unknown password, have an IP block active, or cannot be reached by the Snare Server.

Note: If an Agent is in this group, then there was no way to check the version string or Agent type. This means that Agents which would be ignored by these two filters may show up in here until they can be contacted successfully.

4.1.4. Agents ignored by version string filter.

These Agents were ignored because their version string did not match the specified version string in the configuration.

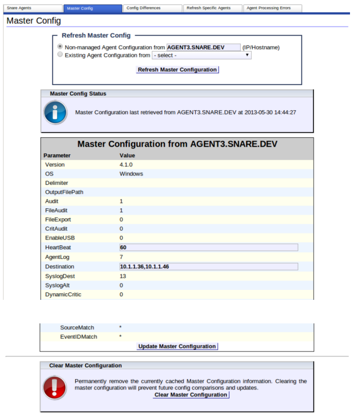
4.1.5. Agents ignored by hostname filter.

These Agents were ignored because their hostname did not match the specified hostname filter.

4.1.6. Agents ignored by type filter.

These Agents were ignored because they did not match the Agent Type selection (I.e. Snare Agent for Windows v4.1.0, etc).

4.2. Master Config



Master Config

Refresh Master Config

● Non-managed Agent Configuration from AGENT3.SNARE.DEV (IP/Hostname)
○ Existing Agent Configuration from - select - ▾

Refresh Master Configuration

Master Config Status

Master Configuration last retrieved from AGENT3.SNARE.DEV at 2013-05-30 14:44:27

Master Configuration from AGENT3.SNARE.DEV

Parameter	Value
Version	4.1.0
OS	Windows
Delimiter	
OutputFilePath	
Audit	1
FileAudit	1
FileExport	0
CritAudit	0
EnableUSB	0
HeartBeat	60
AgentLog	7
Destination	10.1.1.36,10.1.1.46
SyslogDest	13
SyslogAlt	0
DynamicCritic	0
SourceMatch	*
EventIDMatch	*

Update Master Configuration

Clear Master Configuration

Permanently remove the currently cached Master Configuration information. Clearing the master configuration will prevent future config comparisons and updates.

Clear Master Configuration

The Master Config tab provides the ability to specify the Agent that the Master Configuration is imported from.

At the top is the *Refresh Master Config* option box. You can set it to either refresh the Agent Configuration from a custom IP Address or Hostname, or by selecting one of the managed Agents from the dropdown box.

Once you select the Agent to retrieve the config from, click the *Refresh Master Configuration* button. The objective will retrieve the latest copy of the Master configuration.

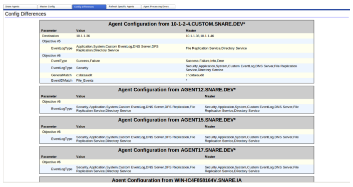
Note: Refreshing the Master Config does **not** compare the configuration with the managed Agents. To do this you need to run the *Regenerate* option again.

Also note: The Master Config is cached locally and is only refreshed manually. This means you can take the Master Agent offline or make changes to it and safely *Regenerate* the objective without it affecting the Master Configuration.

Once you have refreshed the Master Configuration, it will be listed in full on the page so you can review it to ensure it is what is required. Some Agent Types have a couple of useful fields (like the Destination Address) that are allowed to be edited within this interface. You can make your changes and use the *Update Master Configuration* button to save it. This is not pushed out to the Master Agent, and will be lost if the Master Config is refreshed again.

Finally, it is also possible to clear out the Master Configuration by using the option at the very bottom of the page. This is useful if a bad config has been loaded, and you wish to remove it as a precaution before setting up a working config and refreshing it.

4.3. Config Differences



Config Differences

Agent Configuration from 10-1-2-4.CUSTOM.SNARE.DEV*

Parameter	Value	Master
Destination	10.1.1.36	10.1.1.36,10.1.1.46
Objective #5		
EventLogType	Application,System,Custom EventLog,DNS Server,DFS Replication,Directory Service	File Replication Service,Directory Service
Objective #6		
EventType	Success,Failure	Success,Failure,Info,Error
EventLogType	Security	Security,Application,System,Custom EventLog,DNS Server,File Replication Service,Directory Service
GeneralMatch	c:dataaudit	c:\data\audit
EventIDMatch	File_Events	*

Agent Configuration from AGENT12.SNARE.DEV*

Parameter	Value	Master
Objective #6		
EventLogType	Security,Application,System,Custom EventLog,DNS Server,DFS Replication,File Replication Service,Directory Service	Security,Application,System,Custom EventLog,DNS Server,File Replication Service,Directory Service

Agent Configuration from AGENT15.SNARE.DEV*

Parameter	Value	Master
Objective #6		
EventLogType	Security,Application,System,Custom EventLog,DNS Server,DFS Replication,File Replication Service,Directory Service	Security,Application,System,Custom EventLog,DNS Server,File Replication Service,Directory Service

Agent Configuration from AGENT17.SNARE.DEV*

Parameter	Value	Master
Objective #6		
EventLogType	Security,Application,System,Custom EventLog,DNS Server,DFS Replication,File Replication Service,Directory Service	Security,Application,System,Custom EventLog,DNS Server,File Replication Service,Directory Service

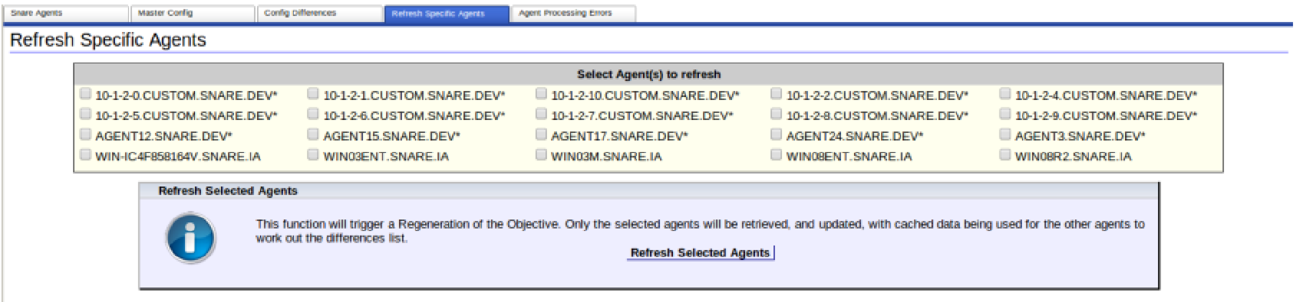
Agent Configuration from WIN-IC4F858164V.SNARE.IA

The Config Differences tab is only displayed when there are differences between the Master Configuration and the managed Agent configurations. It lists each Agent with differences, and only shows the fields that do not match. All other fields are the same as the Master Configuration.

This is the best place to check when there are configuration differences reported between the Agents. It should make the process of checking the differences and resolving them quite easy.

If a *Push* is attempted on an Agent type that does not support it, then it will also be listed on this page.

4.4. Refresh Specific Agents



Refresh Specific Agents

Select Agent(s) to refresh

□ 10-1-2-0.CUSTOM.SNARE.DEV*	□ 10-1-2-1.CUSTOM.SNARE.DEV*	□ 10-1-2-10.CUSTOM.SNARE.DEV*	□ 10-1-2-2.CUSTOM.SNARE.DEV*	□ 10-1-2-4.CUSTOM.SNARE.DEV*
□ 10-1-2-5.CUSTOM.SNARE.DEV*	□ 10-1-2-6.CUSTOM.SNARE.DEV*	□ 10-1-2-7.CUSTOM.SNARE.DEV*	□ 10-1-2-8.CUSTOM.SNARE.DEV*	□ 10-1-2-9.CUSTOM.SNARE.DEV*
□ AGENT12.SNARE.DEV*	□ AGENT15.SNARE.DEV*	□ AGENT17.SNARE.DEV*	□ AGENT24.SNARE.DEV*	□ AGENT3.SNARE.DEV*
□ WIN-IC4F858164V.SNARE.IA	□ WIN03ENT.SNARE.IA	□ WIN03M.SNARE.IA	□ WIN08ENT.SNARE.IA	□ WIN08R2.SNARE.IA

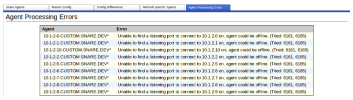
Refresh Selected Agents

This function will trigger a Regeneration of the Objective. Only the selected agents will be retrieved, and updated, with cached data being used for the other agents to work out the differences list.

Normally when the *Regenerate* option is selected the objective will refresh every managed Agent. When you are managing a large number of Agents, this can take a while. To get around this, you can select only those Agent(s) that you wish to refresh. The system will then regenerate only these Agents, and use the cache for all the others.

This is quite useful for testing or fixing up a problem with a specific Agent.

4.5. Agent Processing Errors



Agent Processing Errors

Agent	Error
10-1-2-0.CUSTOM.SNARE.DEV*	Unable to find a listening port to connect to 10.1.2.0 on, agent could be offline. (Tried: 6161, 6165)
10-1-2-1.CUSTOM.SNARE.DEV*	Unable to find a listening port to connect to 10.1.2.1 on, agent could be offline. (Tried: 6161, 6165)
10-1-2-10.CUSTOM.SNARE.DEV*	Unable to find a listening port to connect to 10.1.2.10 on, agent could be offline. (Tried: 6161, 6165)
10-1-2-2.CUSTOM.SNARE.DEV*	Unable to find a listening port to connect to 10.1.2.2 on, agent could be offline. (Tried: 6161, 6165)
10-1-2-5.CUSTOM.SNARE.DEV*	Unable to find a listening port to connect to 10.1.2.5 on, agent could be offline. (Tried: 6161, 6165)
10-1-2-6.CUSTOM.SNARE.DEV*	Unable to find a listening port to connect to 10.1.2.6 on, agent could be offline. (Tried: 6161, 6165)
10-1-2-7.CUSTOM.SNARE.DEV*	Unable to find a listening port to connect to 10.1.2.7 on, agent could be offline. (Tried: 6161, 6165)
10-1-2-8.CUSTOM.SNARE.DEV*	Unable to find a listening port to connect to 10.1.2.8 on, agent could be offline. (Tried: 6161, 6165)
10-1-2-9.CUSTOM.SNARE.DEV*	Unable to find a listening port to connect to 10.1.2.9 on, agent could be offline. (Tried: 6161, 6165)

This tab will be generated only when there are problems communicating with Agents during the regeneration process, and they will be listed here.

This is the place to check when an Agent is marked as uncontactable, since it will be listed with the reason next to it.

5. Troubleshooting

5.1. Agent Processing Errors

These are the common errors that may be encountered when attempting to communicate with Snare Agents.

5.1.1. Unable to push config to agent version.

The version of the Snare Agent installed does not support pushing config. You will need to manually update it to correct configuration differences.

5.1.2. Could not resolve an IP address, unable to communicate with agent.

The Console was unable to find an IP address to use to communicate with the Agent. Please configure your DNS server, or update the server hostname, to allow it to find a valid IP address.

5.1.3. Unable to find a listening port to connect to [ipaddress] on, agent could be offline.

The Console knows what IP address to use for the Agent, but none of the port numbers provided are valid. Please verify that the port configured on the Agent is the same as the one configured within the Console and that there are no firewalls or IP blocks preventing a connection.

5.1.4. Unable to find a password to authenticate to.

The Console is able to find the Agent and the right port, however, none of the passwords specified in the console are working. Please verify the Agent password is listed in the Snare Configuration Wizard, or the Agent Management Console.

5.2. Debugging

When debugging communication problems between the Console and the Agent, there are a couple of things to check:

1. The network allows communications from the Server to the Agent.
2. The Agent has Remote Management enabled.
3. The Remote Management port matches the port configured in the Console.
4. The Remote Management password matches the password configured in the Console.
5. You are using a supported Snare Agent version.

5.3. Why are there more "Agents" listed than I can manage?

Every device that reports data to the Snare Server will be listed on the *Snare Agents* page in one of the status groups, even the devices that aren't compatible Snare Agents. This is because the Snare Server cannot identify compatible Snare Agents from other devices when they are reporting data to the Server. As a result, they are all processed using the type, hostname, and version filters specified for the management objective, and will be discounted for the most appropriate version.

It's quite common for syslog servers, or the Snare Browser Agents, to be listed on this page even though they cannot be managed. You can safely ignore these extra devices listed on this page, and after a device hasn't reported to the Server for over 3 months, it will be removed from the list.