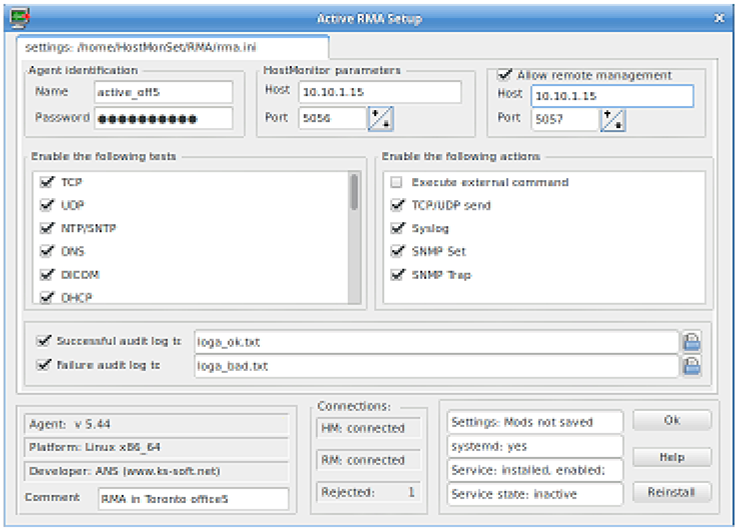
Active RMA for Linux: settings

More information on www.ks-soft.net

[Active RMA for Linux](#)
[How to install service](#)
[Console version parameters](#)
[How upgrade old agents remotely](#)

Agent identification



settings: /home/HostMonSet/RMA/rma.ini

Agent identification
Name: active_off5
Password: ●●●●●●●●●●●

HostMonitor parameters
Host: 10.10.1.15
Port: 5056

☑ Allow remote management
Host: 10.10.1.15
Port: 5057

Enable the following tests
☑ TCP
☑ UDP
☑ NTP/SNTP
☑ DNS
☑ DICOM
☑ DHCP

Enable the following actions
☐ Execute external command
☑ TCP/UDP send
☑ Syslog
☑ SNMP Set
☑ SNMP Trap

☑ Successful audit log to: logs_ok.txt
☑ Failure audit log to: logs_bad.txt

Agent: v 5.44
Platform: Linux x86_64
Developer: ANS (www.ks-soft.net)
Comment: RMA in Toronto office5

Connections:
HM: connected
RM: connected
Rejected: 1

Settings: Mods not saved
systemd: yes
Service: installed, enabled;
Service state: inactive

- **Name**

  Unique name that identifies an agent. You should not assign the same name for several agents. If you do so, HostMonitor will accept connection from 1st started agent and reject connection from other agents with the same name

- **Password**
  Minimum six-character length password. An empty password using is not permitted. Several RMA agents may use the same password. The password is required for every communication session between RMA and HostMonitor or RMA and RMA Manager. All traffic between RMA and HostMonitor or RMA and RMA Manager is encrypted and the password itself is never transmitted through the network without encryption.

Note: when you setup agent record using [HostMonitor](#) or [RMA Manager](#) GUI, you should use exactly the same name and password that were used when you setup Active RMA on remote system using rma_cfg utility.

HostMonitor parameters

- **Host**
- **Port**

These parameters specify where HostMonitor is running and what TCP port should be used for connection.

Allow remote management

- **Host**
- **Port**

If you enable remote management, you should specify IP address or hostname of the system where RMA Manager is running. RMA Manager and HostMonitor can be started on the same system. In this case you should use different TCP ports for connection. Default settings: HostMonitor listens for incoming connections from RMA on TCP port 5056, while RMA Manager utilizes port 5057.

Note1: It is not necessary to have RMA Manager running all the time. If RMA cannot connect to RMA Manager it will try to establish communication every 30 sec.

Note2: If you start RMA Manager on the same system where HostMonitor is running, HostMonitor tells all connected RMA to establish connection with RMA Manager immediately (if "Full management" option is enabled for the agent).

Restrictions

- **Enable the following tests**
  specifies the list of tests methods allowed for execution by this RMA. To enable a test mark the corresponding check box, to disable a test unmark the box near it.
- **Enable the following actions**
  specifies the list of actions allowed for execution by the agent. To enable a action mark the corresponding check box, to disable a action unmark the box near it.

Logging

- **Successful audit log to**

  here you may specify a log file where agent will store information about successfully accepted connections. This log has no use when everything works well (it then just takes space on the hard drive), but you may found it really helpful when a sophisticated network problem has to be fixed. If you specify just the name of the file (without a full path), an agent will store a log in the same directory where it was started from.
- **Failure audit log to**

  you may specify another log file where an agent will store information about rejected requests. E.g.: connections from an IP addresses that are not allowed or connections with invalid password, etc. Log file is a simple text file that contains date of the event, remote IP address from which an attempt of connection has occurred and information about the error. If you specify just the file name (without path), an agent will store it in the directory where it was started from.

The lower part of the configuration window mostly contains information about an agent. Those fields (from the top to the bottom of the window) are joined into three groups: Agent information, Statistics and Agent status.

Agent information:

- You are not able to change information shown in grey fields: agent version, OS platform, developer information
- Comment: Here you may provide any text that will help you to identify agent (useful when you are monitoring 100 LANs using 100 RMA agents). HostMonitor and RMA Manager will display the content of these fields when they work with remote agents.

Agent status

Here you may check is systemd detected; is rma_active installed as service; is service running (active). You may install service or reinstall service if rma_active module and/or ini files were moved to different location. Also here you can check the state of currently edited agent configuration i.e.: are the changes for the current configuration already saved or not.