

GWAVA Inc.

# Retain for Social Media

---

## Installation and configuration Guide

“GWAVA” is a registered trade mark of GWAVA Inc, 100 Alexis Nihon, Suite 500, Saint Laurent, Quebec H4M 2P1

Retain” is a trade mark of GWAVA Inc, 100 Alexis Nihon, Suite 500, Saint Laurent, Quebec H4M 2P1

Exchange and Windows are trademarks of Microsoft Inc.

All other trademarks are the property of their respective owners.

## Contents

Setting up the VM & Installing the OS .....	3
Before setting up the Virtual Machine .....	3
Configure the Virtual Machine.....	3
RSM Configuration .....	5
Proxy Configuration .....	5
RSM CA Certificate Installation .....	6
Social Information Governance Configuration .....	6
Social Information Governance Rules & Actions .....	6
Enabling Social Information Governance.....	7
Creating Pre-defined Social Information Governance Rules and Actions .....	7
Creating Custom Social Information Governance Rules .....	7
Creating Custom Social Information Governance Actions.....	7
Social Information Governance Moderation .....	8
Creating a Moderation Queue .....	8
Creating a Moderation Action .....	8
Configuring Secure Social Media Authentication .....	8
Configuring RSM to authenticate to a company's social media site .....	9

All installation and base configuration is described here. In addition, in-program help and documentation may be found by linking to the online knowledge base, accessed through the Retain for Social Messaging Gateway interface. This link is found in the top right hand corner of the interface.

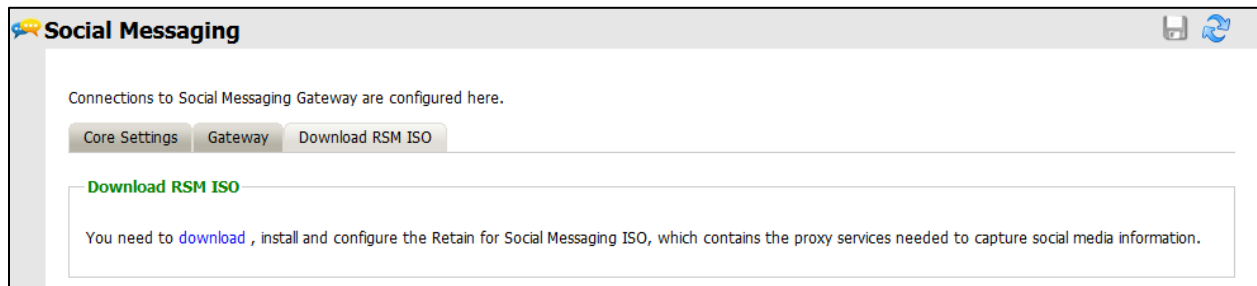
## Setting up the VM & Installing the OS

### Before setting up the Virtual Machine

- Ensure the firewall is configured as such:
  - From RSM WAN IP to Untrusted, all TCP/UDP ports
  - If the RSM WAN IP is a private IP, it needs to be NATed to an appropriate routable IP address. The LAN IP address does not need a corresponding inbound NAT rule.
- **NOTE:** It is critical that these firewall rules are in place before proceeding.

### Configure the Virtual Machine


1. Download the ISO from the link found in the Social module page, on the 'Download RSM ISO' tab.



2. Install it onto a VM or to the desired machine with the following minimum specs
  - a. 2GB RAM (minimum)
  - b. 2 CPU cores (minimum)
  - c. 60 HDD (minimum)

The recommended RAM, CPU and HDD specification will be determined by the expected load and size of the organization being served. Consult your GWAVA technical representative.

  - d. 2 NICs - vmxnet 3, ensuring the interfaces are in different VLANs. NOTE: The second NIC in the VMware settings list is the primary NIC that will be used for proxy traffic. This NIC will be labeled "Internet" on the RSM. The first NIC will be the "Local" port, and may be disconnected if desired when configured.
  - e. Redhat Linux enterprise 5 64bit base OS (selected from the dropdown list when setting up the VM – there is no need to actually install the Redhat OS)
3. Mount the ISO and start up the VM or server.
4. Set the password for the "tech" and "admin" users. This will then install the RSM OS. Once it's installed and has come back up after the reboot, the RSM will have the default LAN IP of 192.168.0.254/24. The WAN interface will try to obtain an IP address from DHCP.
5. Set the LAN IP via the console by sending a ctrl-alt-ins and then follow the prompts.
6. All configuration operations are via the web user interface. Log onto the RSM interface by browsing to the LAN IP on either port 80 or 443 and logging in as the "tech" user, (the "admin" user doesn't have the required permissions).




# Retain

Login to Retain for Social Media

Login

You will initially be prompted to confirm the EULA and provide your details. If the email address is not accepted at this stage (the RSM will try to validate all addresses), then use “root@ mail.RSM”.



# Retain

Wizard

Home

Access Policies

Webmail

Users & Groups

Administration

Reporting

Network Monitoring

Content Scanning

Workstation Agent

Social Media

Internet Auth

Internet Quotas

Advanced Firewall

Traffic Shaping

Configuration

User: tech [logout]

## Retain for Social Media Home

Current Internet Link Information	
State	Up
IP Address	10.1.0.62
<a href="#">More Information</a>	

Firmware Version	
Release	Mercury (29.4.2)
Date installed	Tue 25 Nov 2014 14:37:56
Update expiry date	Sat 28 Feb 2015
<a href="#">More Information</a>	

Retain for Social Media Model	
The model of your Retain for Social Media	30

Current Modules
Remember: To access your Retain for Social Media from anywhere on the Internet you can use the following address <b>gwava-qa-rick3.safenetbox.biz</b>

- Click the “Wizard” button from the left-hand navigation bar, and follow the prompts for setting the language, time zone and network details.

8. Once the network settings have been accepted, select **Configuration ->Internet** from the left hand navigation pane, and check **"Show Advanced Options"**.
  - a. From the dropdown list next to "DNS server configuration" select "Always use static server" and then enter in the required DNS servers.
  - b. Click on Update.
  - c. Browse to **Configuration -> Apply** and click on the **"Apply Changes"** button.

**PLEASE NOTE:**

- If the LAN IP Address has been changed in the Wizard setup, you will need to browse to the new IP address and log onto the RSM interface again after applying the network settings.
  - The WAN (or Internet) Interface of the RSM will be used for proxy traffic.
  - The LAN interface is not used for production traffic, but can be utilized as a management-type port if required.
  - It is **critical** that the two interfaces are configured on different subnets from this point on, regardless if the LAN port is utilized or not.
9. After the Network configuration has been completed you will be prompted to supply a sitekey. A sitekey is a unique identifier for your RSM and it should be relevant to your organization. Only alphanumeric and "-" are accepted, with a minimum character count of 3.
    - a. Your RSM Blue representative will supply the registration key to you.
    - b. After the sitekey has been successfully applied, your RSM will reboot.
  10. Log back onto the RSM and browse to **Administration -> Updates** and click on "Run Update Now".

The RSM will go through its update process, which could take up to 30 minutes and reboot multiple times.

## RSM Configuration

The configuration of the RSM is achieved via its Web User Interface. You need only browse to the (WAN or LAN) IP address and enter in the appropriate credentials. For the following you will need to use the "tech" account with the password that was set when creating the virtual machine.

**NOTE:** When making changes to the RSM configuration, remember to update the page you are working on before navigating away from it. When you want to make your changes live, browse to the "Apply" section in the relevant module and click on the "Apply Changes" button.

## Proxy Configuration

The following describes how to configure the RSM in a direct proxy setup. The client will then direct their browser to the WAN IP address of the RSM on the specified port (8080 for example).

1. Browse to Configuration -> Web Proxy.
2. In the dropdown list next to "Direct Proxy Mode" select "Direct".
3. Specify the port to use (8080 by default).
4. In the dropdown list next to "Provide proxy on Internet interface", select "yes".
5. In the dropdown list next to "HTTPS inspection", select "Enabled for all traffic".
6. Click on "Update".
7. Browse to Configuration -> Apply and click on the "Apply Changes" button.

8. After 1-2 minutes, once the changes have been applied (when the yellow apply banner disappears), test the proxy by pointing your browser to the RSM WAN IP on the specified port and browse to a standard HTTP web site (HTTPS sites will be tested shortly).NOTE: You can view the proxy logs by browsing to Configuration -> Web Proxy and clicking the “View Web Proxy logs” link in the top right hand corner of the page.

## RSM CA Certificate Installation

The RSM will be performing HTTPS inspection, meaning it will have visibility to view encrypted web traffic. This is critical to ensure that all Social Information Governance functionality is available. In order to do this successfully, the RSM CA Certificate needs to be installed on all client devices that will be using the RSM as a proxy service.

1. Download the certificate from <http://<WAN IP>/noauth/cacert>.
2. If using Microsoft Active Directory create a Group Policy Object
  - a. In GPMC open the relevant policies that apply to the Computers that need to have this certificate installed and navigate to Computer Config>Windows Settings>Security Settings>Public Key Policies and import the CA Certificate as a Trusted Root Authority.

**NOTE:** This GPO will NOT apply to Safari or Firefox browsers. The certificate will need to be manually installed.

3. If manually installing the certificate ensure it's installed as a Trusted Root certificate.
4. Once the certificate has been deployed, test by browsing to a HTTPS site and view the web proxy logs. You should not see a certificate warning in the browser and the proxy logs should display your HTTPS request.

## Social Information Governance Configuration

### Social Information Governance Rules & Actions

Social Information Governance is a Rule/ Action process, meaning that a rule needs to be triggered before an action takes place. A rule is made up of one or more criteria. A criterion tells the RSM what should trigger the rule. A rule has one action assigned to it. An action may have multiple sub-actions.

Actions can be either:

- Block
- Alert
- Modify
- Moderate
- Or in some cases, combinations of the above (i.e., Block and Alert) For example a rule to block a staff member from posting extreme profanity on twitter will contain the following:
  - A criterion that uses the “extreme profanity” pattern list.
  - Another criterion that sets the Application type to “Twitter”.
  - A final criterion that specifies the user's action as “send”
  - An action to block.

**NOTE:** *All Criteria must be true before the rule is triggered.* In other words: If the user **sends** a post to **Twitter**, which matches an entry in the “**extreme profanity**” pattern list, then take the associated action to **Block**. This rule would not trigger if the user **read** extreme profanity on Twitter, so care must be taken in establishing the Social Information Governance requirements for your organization. The RSM comes with predefined rules that may apply to the relevant organization type.

## Enabling Social Information Governance

1. Enable Social Information Governance by browsing to **Content Scanning -> General**. Under the **SafeChat Settings** table:
  - a. From the dropdown list next to "Enable SafeChat scanning of web content?" select "Yes"
2. Click on "Update"
3. Browse to **Content Scanning -> Apply** and click on the "Apply Changes" button.

## Creating Pre-defined Social Information Governance Rules and Actions

1. After the changes have been applied create the predefined rules by browsing to **Content Scanning -> General** and click on the "Add suggested settings" button.
2. Browse to **Content Scanning -> Rules** where you can see the rules that have been created. The rules and corresponding actions will be currently disabled.
3. Enable the rules by
  - a. Clicking "edit" next to the rule.
  - b. Check "Enabled".
  - c. Additional criteria can be added at this stage by clicking on the "Add Criteria" link.
  - d. Click on "Update".
4. When you are happy for the rules to come into effect, browse to **Content Scanning -> Apply** and click the "Apply Changes" button.

## Creating Custom Social Information Governance Rules

To add or modify a rule:

1. Browse to **Content Scanning -> Rules** and click on "Add new rule" in the top left hand corner
2. Enter a descriptive name for the rule into the textbox provided. This will be used for referring to this rule, for example when modifying or deleting this rule.
3. Select the action to be run when the rule is matched.
4. Click the Update button to save the rule.
5. Enter criteria as required. The rule will be triggered when all of the listed criteria are matched.  
**NOTE:** If no criteria are specified then this rule will never be triggered.
6. Select the checkbox provided at the top of the page to enable the rule, once you are happy for it to become active.
7. Click the Update button to save the rule.

## Creating Custom Social Information Governance Actions

To add or modify an action:

1. Enter a descriptive name for the action into the textbox provided. This will be used for referring to this action, for example when modifying, deleting or using this action.
2. Click the Update button to save the action.
3. Enter sub-actions as required.  
**NOTE:** If no sub-actions are specified then this action will not do anything, but the rule will still trigger a match, this can be useful for reporting.
4. Select the checkbox provided at the top of the page to enable the action, once you are happy for it to become active.
5. Click the Update button to save the action. Once all changes have been made to the **Content Scanning** section:
  - a. Browse to **Content Scanning -> Apply**.

- b. Click on the “Apply Changes” button.

The Configured Social Information Governance rules and actions will now be live in a few seconds.

## Social Information Governance Moderation

The Moderation section of Content Scanning allows authorized users to approve or deny messages held by a “Hold for Moderation” sub-action. A Content Scanning action needs to be configured to hold messages in a particular moderation “queue” until processed. An authorized user can then view each queue, reviewing the pending messages of a queue in detail, and selecting whether each message is approved or denied. An example would be to hold for moderation any messages that contain the name of the company for moderation and review before it’s sent to Twitter, Facebook, etc. The authorized user can then elect to allow that message to be sent or reject the message, giving an explanatory comment if necessary.

**NOTE:** Please refer to the online help under **Users & Groups** to create individual users and groups if you want to limit access to these features a defined group of users. Social Information Governance Moderation requires the configuration of:

1. A moderation queue and;
2. An action to hold messages in the moderation queue.

## Creating a Moderation Queue

1. Browse to **Content Scanning -> Manage Moderation Queues**.
2. Select “Create New Queue”.
  - a. Provide a descriptive name for the queue.
  - b. Select which groups (if any) can view this queue.
  - c. If an explanatory comment is required for any actions within this queue (i.e., releasing or denying), set the appropriate value here.
4. Click on “Update”.

## Creating a Moderation Action

This is simply a Content Scanning action to hold messages into the specified moderation queue.

1. Follow the steps described under “Creating Custom Social Information Governance Actions”.
2. When selecting the sub-action, select “Hold for Moderation”.
3. Select the moderation queue from the dropdown list.
4. Assign this action to the required rule (please refer to “Creating Custom Social Information Governance rules” for more detail).

## Configuring Secure Social Media Authentication

The RSM can be used to grant users access to social media accounts without having to divulge the account password. The RSM will determine whether users can access particular social media accounts based on the group membership of the user. This can be used, for example, to allow certain members of your organization the ability to make posts to your organization’s Twitter or Facebook account without divulging the password for those accounts.

**NOTE:** This functionality currently applies to LinkedIn, Twitter and Facebook accounts.

## Configuring RSM to authenticate to a company's social media site

1. Browse to **Social Media -> Accounts** and click on "Configure New Account" in the top right hand corner of the page.
2. Configure the account options:
  - a. Select the application.
  - b. Type in the username and password for the account

**NOTE:** This feature will not work with accounts that require two-factor authentication. It is recommended that a long, complex and very secure password be used for the account.

- c. Select which user groups can access this account through the RSM.

**NOTE:** Users with Social Media Account administration privileges are allowed to access all social media accounts regardless of this setting.

- d. Provide a description of the account (i.e., "ABC Corp. Main Facebook page")
  - e. Set a session lifetime. This determines how long the login session cookie will be active before timing out. Leave it blank to use the application's default values.
3. Click on "Update".
  4. Browse to **Content Scanning -> Apply** and click on the "Apply Changes" button.
  5. Users can access the company's social media sites by browsing to the RSM, supplying appropriate credentials and then browse to **Social Media -> Accounts**.
    - a. They will see the list of social media accounts they have permission to access (for example Facebook and Twitter, but not LinkedIn).
  6. Click on the social media account desired, and the RSM will log into that application for the user.