



MAF ICIMS™ – Security Guide

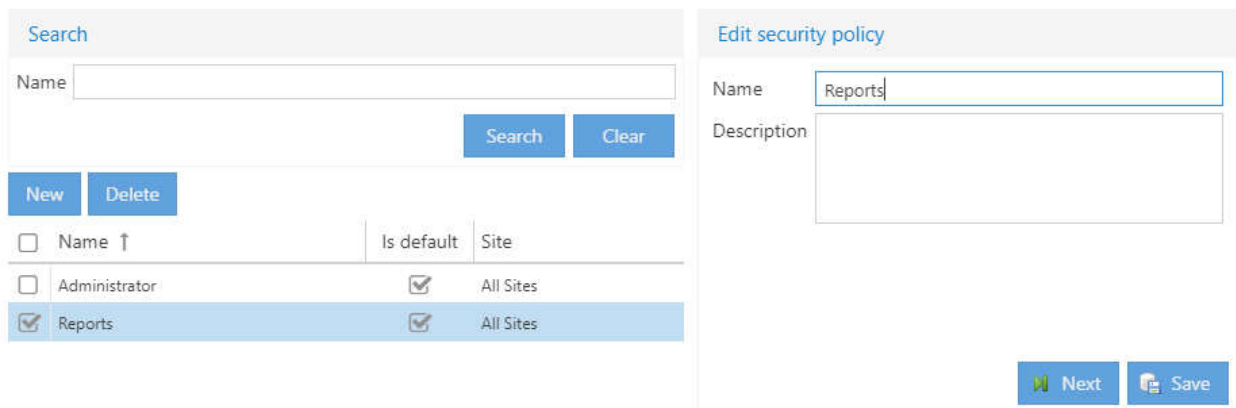
Monitoring and Reporting for Unified Communications



1. Default Security Policies

The *Security Policies* window displays the security group to which a user can be assigned. The Administrator group has unlimited data access, and the Reports group has the most limited data access.

Select *Security Policies* from the Administration menu. The *Security Policies* window is displayed:



The screenshot shows two panels. The left panel, titled "Search", contains a text input field for "Name", "Search" and "Clear" buttons, and "New" and "Delete" buttons. Below is a table with columns "Name", "Is default", and "Site". The right panel, titled "Edit security policy", contains a "Name" input field with "Reports" entered, a "Description" text area, and "Next" and "Save" buttons at the bottom.

<input type="checkbox"/>	Name ↑	Is default	Site
<input type="checkbox"/>	Administrator	<input checked="" type="checkbox"/>	All Sites
<input checked="" type="checkbox"/>	Reports	<input checked="" type="checkbox"/>	All Sites

Enter relevant criteria to search for the relevant items. The following option is available:

Name: Enter the name of the policy you search for.

To view the result of your search, click **Search**. The *Security Policies* window will display the existing policies.

Click **Clear** to delete the information entered to perform a new search.

The Security Policies window already displays the following groups:

Administrators

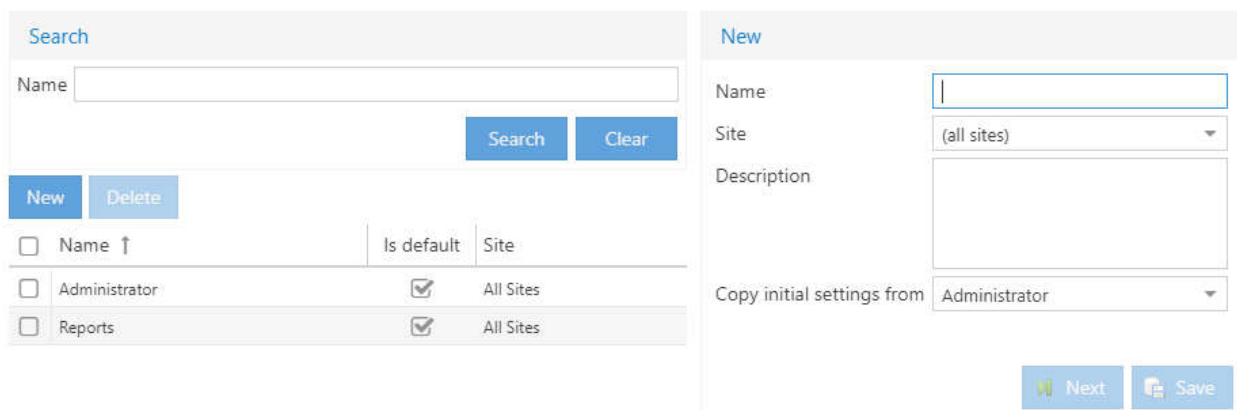
This is the **highest security** group. Administrators can **access all parts** of MAF ICIMS.

Reports

This is the second security policy. Reports users have access **only** to the Reports module (Report Builder, Standard Reports and Capacity Reports).

2. Adding a New Group

Click New to add a new policy. The following window is displayed:



The screenshot shows two side-by-side panels. The left panel, titled 'Search', contains a search bar with the text 'Name' and a search button. Below the search bar are 'New' and 'Delete' buttons. A table below shows a list of policies:

<input type="checkbox"/>	Name ↑	Is default	Site
<input type="checkbox"/>	Administrator	<input checked="" type="checkbox"/>	All Sites
<input type="checkbox"/>	Reports	<input checked="" type="checkbox"/>	All Sites

The right panel, titled 'New', contains a form with the following fields:

- Name:
- Site:
- Description:
- Copy initial settings from:

At the bottom right of the 'New' panel are 'Next' and 'Save' buttons.

Enter the following information:

- **Name:** type a name for the new policy
- **Site:** select the site you want to define the policy (leave all for all sites)

- **Description:** type a description for the policy
- **Copy initial settings from:** you can start with options from an already defined policy
- **Policies tree:** In the tree you can select the options for the new policy.

Search

Name

Search **Clear**

New **Delete**

<input type="checkbox"/>	Name ↑	Is default	Site
<input type="checkbox"/>	Administrator	<input checked="" type="checkbox"/>	All Sites
<input type="checkbox"/>	Reports	<input checked="" type="checkbox"/>	All Sites

New

Expand all **Collapse all**

- ▶ Administration
- ▶ Alarms
- ▶ Budget
- ▶ Client rights
- ▶ Dashboard
- ▶ Extended rights
- ▶ Health monitor
- ▶ IM Transcripts
- ▶ Number Management
- ▶ Organization structure
- ▶ Recordings
- ▼ Reports
 - ▶ Capacity reports
 - ▶ Carrier cost comparison
 - ▶ Conference Details
 - ▶ Conference summary
 - ▶ Employee Details
 - ▶ Inactive users
 - ▶ Presence reports
 - ▶ Report builder
 - ▶ Response groups reports

Previous **Save**

Check the rights that will be made **available** to this security policy.

Updating Security Policies

To **edit** the information for an existing security policy, select the policy, and then **you see** in the **right side** the *definition* of the policy.

Enter the necessary changes, and then click **Save** to **save the changes**.

Deleting Security Policies

To **delete** the information for a security policy, select the policy, and then click **Delete**. You will be prompted to **confirm** the **deletion**.

Click **Yes** to **delete the data**, click **No** to **leave the data as it is**.

3. User Management

You can **manage** a list of users of the system.

Each user **is identified with a password and a specific policy**.

This way you can provide access to a range of personnel with different needs, without jeopardizing data security.

Select **Users** from the **Administration-> Security** menu. The **Users** window is displayed:

Search

Name

Status (all) ▼

Security policy

<input type="checkbox"/>	Name	Status	Expiration date	Security policies
<input type="checkbox"/>	admin	Active		Administrator
<input type="checkbox"/>	Graham	Active		Reports
<input type="checkbox"/>	Mark	Active		
<input type="checkbox"/>	Mike	Active		
<input type="checkbox"/>	nhs	Active		

Search

Name	<input type="text"/>
Status	(all) ▼
Security policy	<input type="text"/>

Enter relevant criteria to search for the relevant items.

The **following options** are available:

- **Name:** Enter the name of the user you search for and click **Search**.

The **Users** window will display the existing user(s). Click **Clear** to delete the information entered in order to perform a new search.

- **Status:** Click the drop-down arrow to display the available statuses.
The options are: **Active** and **Locked**.

Select the relevant status for your search or leave the box empty to select all the statuses.

- **Security Policy:** Enter the name of the security policy to search for users assigned to that policy.

To view the result of your search, click **Search**. The **Users** window will display the existing user(s).

Click **Clear** to delete the information entered to perform a new search.

4. Adding a New User

<input type="checkbox"/>	Name	Status	Expiration date	Security policies
<input type="checkbox"/>	admin	Active		Administrator
<input type="checkbox"/>	Graham	Active		Reports
<input type="checkbox"/>	Mark	Active		
<input type="checkbox"/>	Mike	Active		
<input type="checkbox"/>	nhs	Active		

Click **New** to add a new user to the system. The **New User** window is displayed:

New User

Name

New password

Confirm password

Status

E-mail

Sip address

Expiration date

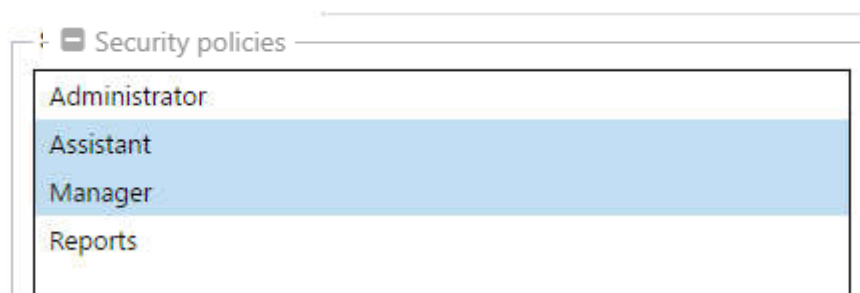
Security policies

Administrator

Reports

Enter the following information:

- **Name:** Type the **Login Name** in this field. The name can consist of alphanumeric characters. The user's first name is a common entry for the Login Name.
- **New Password:** Type the password in this field. The password should consist of at least 6 characters. The password is case-sensitive.
- **Confirm password:** Re-type the password.
- **Status:** select the status of the user: **Active** or **Locked**.
- **Expiration Date:** You can pre-set the user to automatically lock on certain date.
- **Security Policy:** select the relevant policy for the user (you can do multiple selection)



5. Updating Users

To update user parameters, **select** the name of the user to be modified.

Click on the **user**, and the **Update User** window is displayed on the **right side**.

This *window* displays the same fields as the **New User** window.

Enter the necessary changes, and then click **Save** to save the settings. Leave the password fields empty if you do not want to change user's password.

6. Deleting Users

To delete a user from the Users, select the User to be deleted. Click Delete.

When prompted, click **Yes to delete**, or **No** to close the window **without deleting**.

You **cannot delete** the **currently logged in user** (yourself).

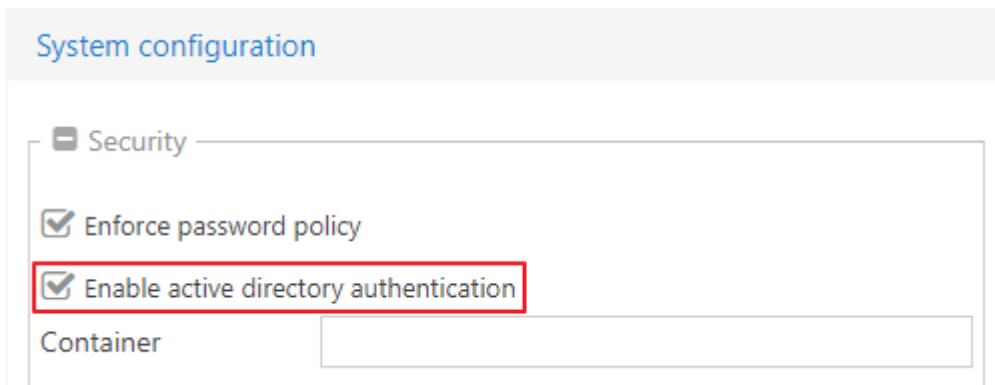
7. Active Directory Authentication

UC Analytics provides the ability for users to automatically login to the system using their Active Directory credentials.

To enable the active directory authentication, follow these steps:

Enable Active Directory Authentication

Proceed to **Administration** -> **System** -> **System configuration** and enable AD authentication by checking the following box:



System configuration

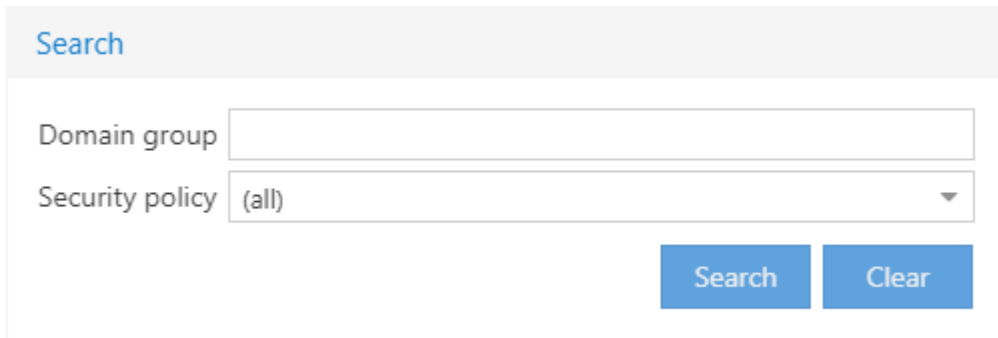
Security

- Enforce password policy
- Enable active directory authentication

Container

Proceed to **Administration** -> **Security** -> **Active directory authentication**.

To search through the active directory group policy we provide the possibility of using the following search criteria's:



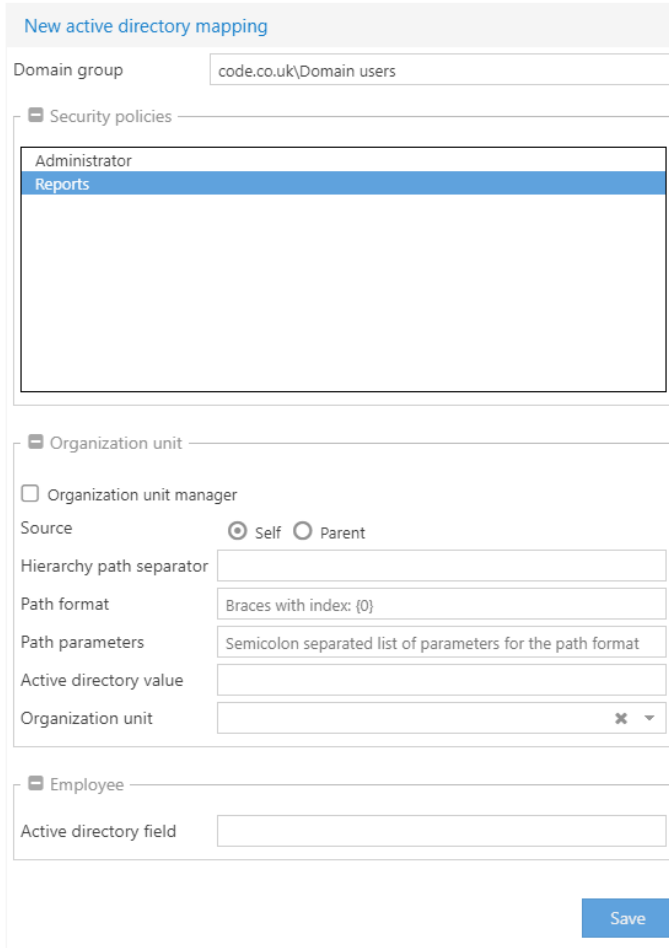
The image shows a search interface with a light gray header containing the word "Search" in blue. Below the header, there are two input fields: "Domain group" with an empty text box, and "Security policy" with a dropdown menu currently showing "(all)". To the right of these fields are two blue buttons: "Search" and "Clear".

- Domain group: Enter the AD group that you are looking for.
- Security policy: select from the dropdown list the security policy that have groups assigned to.

Click **Search** after you have entered the criteria's you are looking for to filter the AD groups

8. Adding AD groups and assigning policies

To enable Active Directory Authentication to the whole AD directory group (all users) click on **New** and enter the following options:



New active directory mapping

Domain group: code.co.uk\Domain users

Security policies

- Administrator
- Reports

Organization unit

Organization unit manager

Source: Self Parent

Hierarchy path separator:

Path format: Braces with index: {0}

Path parameters: Semicolon separated list of parameters for the path format

Active directory value:

Organization unit: x

Employee

Active directory field:

Save

- **Domain group:** domain\Domain Users whereas domain stands for the AD company domain and Domain Users are all the users in the AD.
- **Security policy:** choose from the dropdown the security policy you want to assign to that domain group.

We support the ability of enabling **multiple domain groups** with **different policies** assigned to them by selecting the entering the respective **Domain Group** in the **Domain group** configuration box.

9. Mixed-mode security and logging in as different user

Mixed-mode security

UC Analytics security option permits logging in the system through normal user/password combination **and** through AD authentication in the same time by having **both** users enabled in the Security -> Users and Domain groups enabled in Security -> Active Directory Authentication.

Log in as a different user

To log in the system as a different Active Directory user follow these steps:

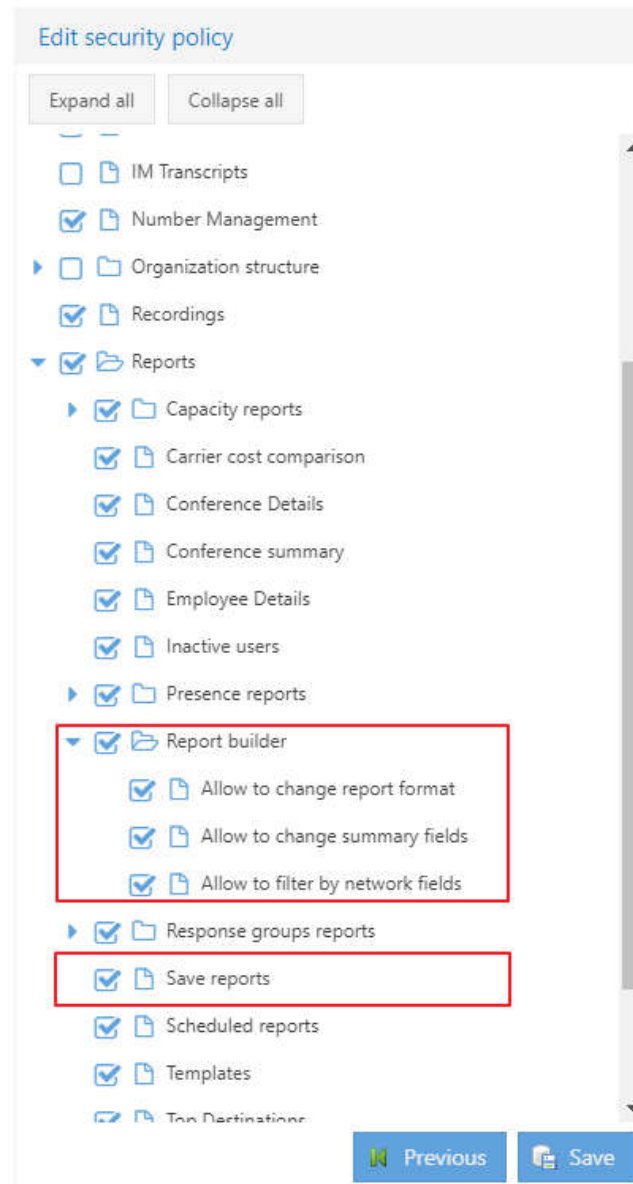
Click on your username in the upper right corner and choose log-out.

In the log in screen you have the ability to both log-in with a normal username/password combination or by clicking “Log in as a different user” and enter domain credentials in the pop-up box.

10. Policy Rights

Report Builder Rights

Report Builder functionality can be further customized per policy to disable the report builder completely or certain functions.



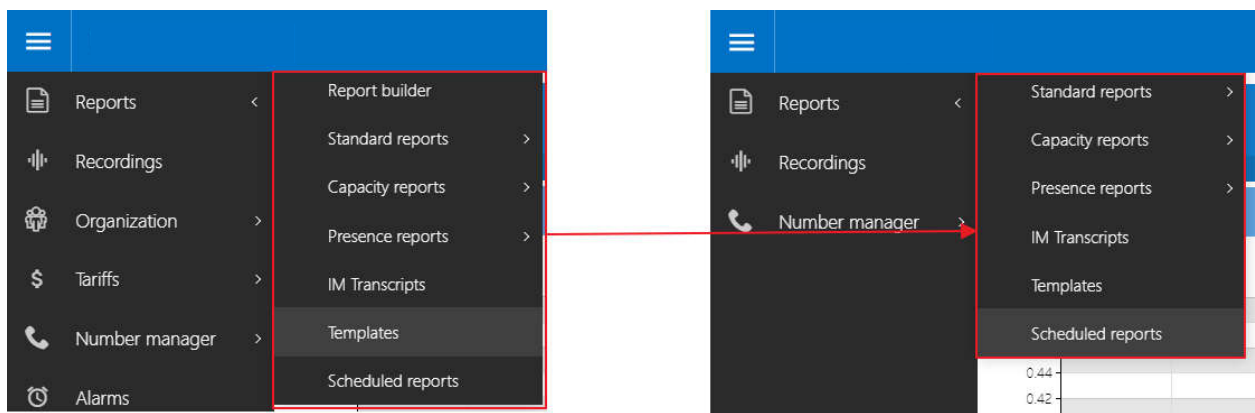
- **Report Builder**
 - **Allow to change report format**
 - **Allow to change summary fields**
 - **Allow to filter by network fields**

Save Reports

By unchecking **Report Builder**, it will completely disable from both the menu system and from the templates section.

Users that have this policy removed will not be able to create a custom report or open for alteration/editing the templates already created.

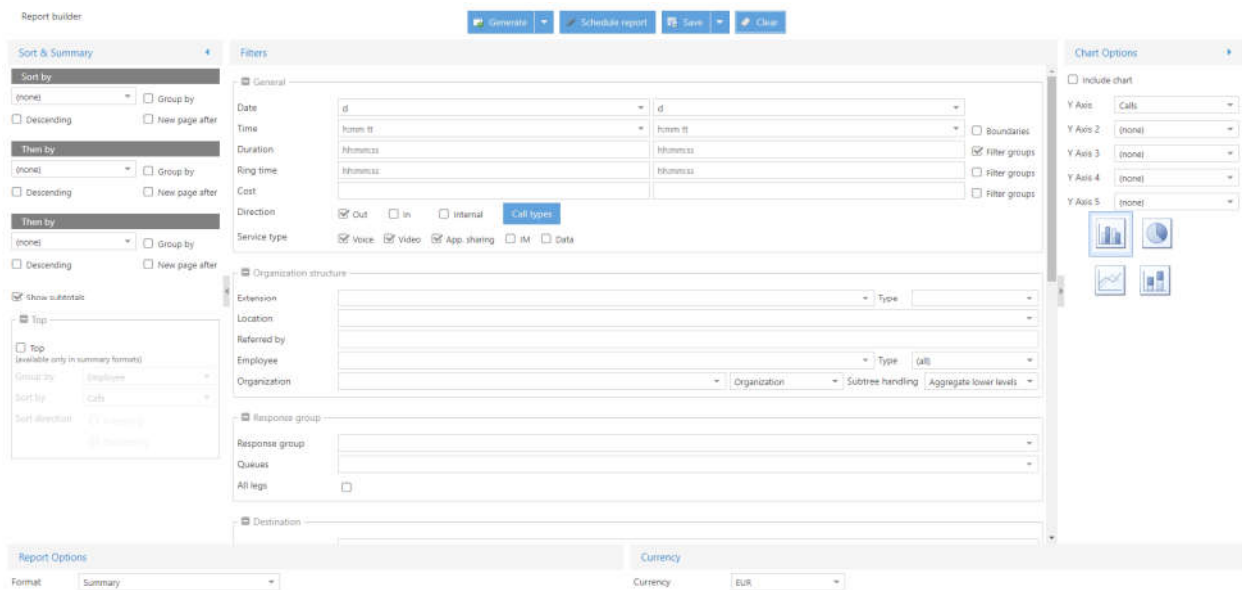
Any other standard reports and/or templates created will still be available to generate.



Further refinements to the report builder functionality can be implemented by removing certain rights.

These will affect the options available in both the report builder and when opening a template for editing:

- **Allow to change report format**
- **Allow to change summary fields**
- **Allow to filter by network fields**



Allow to change report format disables the **Report Options and Currency** section in the lower part of the Report Builder

Allow to change summary fields disables the **Sort & Summary** options in the left area of the Report Builder

Allow to filter by network fields will disable the **network filters** (Lync Fields, Subnet etc.) and will only allow to show the General, Organization Structure, Response Group and Destination fields.

Saving reports templates or overwriting can also be disabled by unchecking **Save Reports** option in the security policies.

Any users affected by the **removal of this policy** will **not be able to save report template** anywhere else but in **Personal** templates section which are only visible to the user itself and will not affect either the original template nor the personal templates created by other users.

Generate Schedule report Save Clear

Filters

General

Date [d] [d]

Time

Duration

Ring time

Cost

Direction

Service type Voice Video App. sharing IM Data

Boundaries
 Filter group:
 Filter group:
 Filter group:
 Filter group:

Save report

Name Response Group Statistics

Report Type Personal

Save Cancel

About MAF InfoCom™

Formed in 2000, MAF InfoCom™ is a leading innovative technology provider with almost 20 years' experience in delivering solutions for Monitoring, Analytics, Reporting and Recording of telephony and Unified Communications, Call Management, Billing & Call Accounting.

We serve tens of thousands customers around the globe, in a large variety of branches. We have installations in over 50 countries ranging from SME's to multi-national global enterprises. In Europe MAF InfoCom™ is the largest provider of UC reporting solutions.

With the market trend towards Unified Communications we expand our sales across the globe rapidly. Our solutions work with every major (IP)PBX and UC manufacturer platform.

Our solutions are offered from the Cloud, On-Premises and Partner Hosted to enable our customers and partners to choose the best model for their needs.

Monitoring, Analytics, Reporting and Recording for Unified Communications.



European Headquarters

Comeniusstraat 2a
1817 MS ALKMAAR
The Netherlands
T: +3172-8200205
E: info@mafinfo.com