Digital Channels Administrator's Guide

Manage personally identifiable information

2/3/2026

Contents

- 

- Administrator

Learn how to assign rules and actions to incoming messages, emails, and workitems to protect your customers' private information.

Related documentation:

-

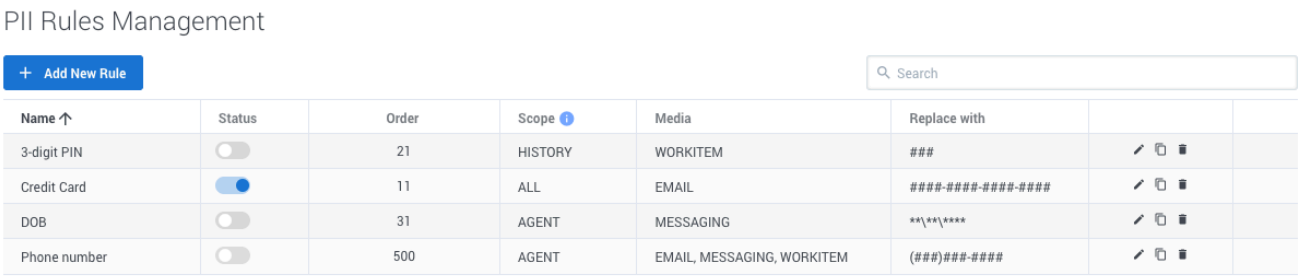
Use PII Rules Management to assign rules to all incoming messages in chat, SMS, WhatsApp, Facebook (private and public messages), Twitter (private and public messages), email, and workitems. These rules use regular expressions to detect private information that you can mask with the replacement text of your choice. For example, you could mask a phone number like this: (###)###-####

> **Important**
>
> Privacy rules are not applied to outgoing messages, such as those sent by a Designer application, an agent, or a bot.

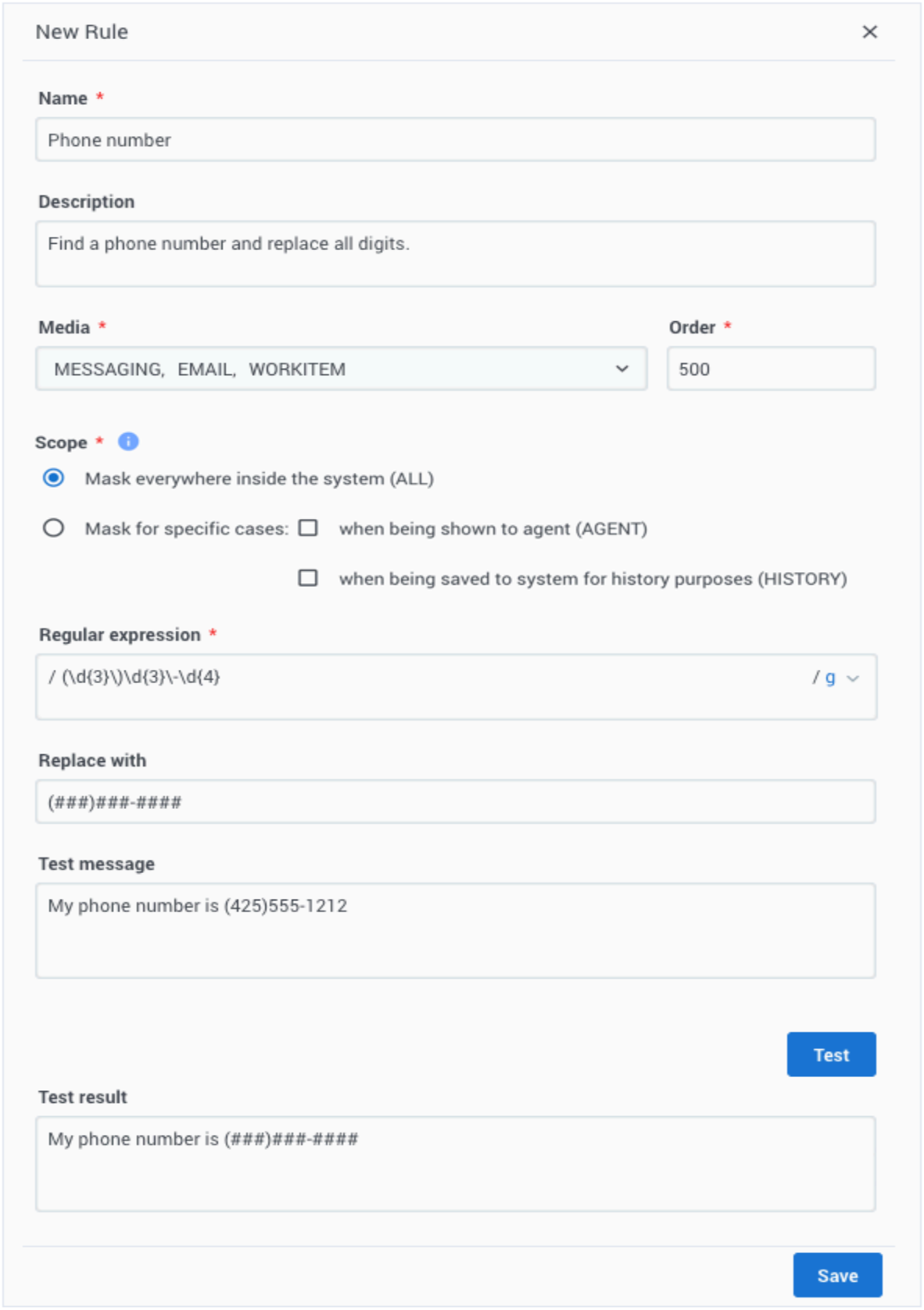
You can create rules for any alphanumeric string that follows a defined pattern represented by a regular expression. When the rule finds a match, it masks the data with a custom-defined string. Here are some common private fields that you can match with a rule:

- Account number
- Credit card number
- Phone number
- Email address
- Date of birth

Access PII Rules Management under the **Privacy** menu.



Create or edit a rule


New Rule
Name *
Phone number
Description
Find a phone number and replace all digits.
Media *
MESSAGING, EMAIL, WORKITEM
Order *
500
Scope *
Mask everywhere inside the system (ALL)
Mask for specific cases:
when being shown to agent (AGENT)
when being saved to system for history purposes (HISTORY)
Regular expression *
/ (\d{3}\)\d{3}\-\d{4}
/ g
Replace with
(###)###-####
Test message
My phone number is (425)555-1212
Test
Test result
My phone number is (###)###-####
Save

When you create a rule, a **New Rule** view opens on the right side of the page. To begin, give your rule a name and a brief description.

Next, choose the types of **Media** for which the the rule should apply. Note: The MESSAGING type represents all chat, SMS, and social media messages.

The **Order** determines the sequence in which rules are applied to the message, starting with the lowest number. The default is 500, but you can choose any value between 0 and 9999. You can also update the order after the rule is saved.

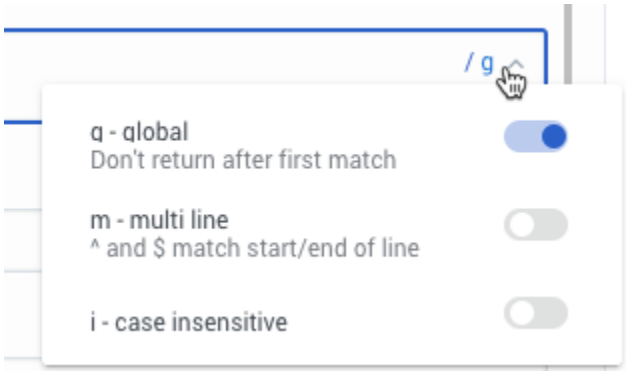
> ### Important
> Genesys does not recommend assigning the same order value to multiple rules in the same scope.

Choose when to apply the rule to the message by selecting the **Scope**. If you mask the data everywhere inside the system (ALL), then the rule is applied right after the user sends a message during the interaction. The data is permanently removed for the message and can't be retrieved later. **If the media is an email or workitem, you must choose this option.**

If you mask for specific cases, then the system treats the data as follows:

- AGENT - The rule is applied when the user's message displays to the agent. The data is saved in the system and can be retrieved later.
- HISTORY - The rule is applied when the message is saved to the system for historical purposes. With asynchronous messages, personal information in the active segment of communication is only visible to the agents who own the active interaction. Personal information in the previous communication segments is hidden.

The **Regular Expression** determines which information to replace in the message. You must use ECMAScript syntax to define the regular expression. The regular expression text area also has a dropdown to set flags for global, multi-line, or case-insensitive searching.



The **Replace with** string is ***** by default. You can change this value to any pattern that makes sense for your use case. For example, it could be (###)###-#### to mask a phone number.

PII Rules Management also supports partial masking.

Finally, don't forget to test your rule before saving.

Test a rule

PII Rules Management includes a testing feature you can use to confirm that the rule is working as expected.

To test, open the rule and enter a **Test message**. When you click **Test**, the **Test result** field shows how your rule handles the test message.

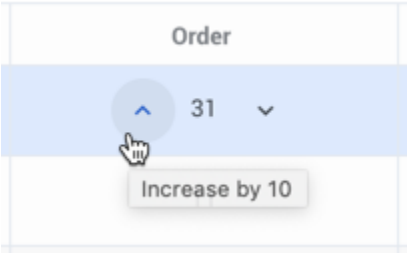
You can adjust your regular expression and replacement text as needed, just remember to click **Save** when you have finished.

Change a rule's status

After you create a rule, you can manage whether it is enabled with the **Status** switch ( ). The switch is off by default, which means the rule is not applied to messages. Any changes to the status take effect immediately.

Reorder a rule

After you create a rule, you can change the order in which it is applied. Hover over the **Order** cell and increase or decrease the value in increments of 10.



Copy a rule

You can copy an existing rule with the **Copy** button ( ). This opens the **New Rule** view with the copied rule information. The name of the rule includes "_*N*", where "*N*" is the number of the copy. For example: Rule_1, Rule_2, and so on.

Delete a rule

To delete a rule, just click the delete icon (🗑). If you just want to disable the rule temporarily, consider changing the rule's status instead.

Best practices

Here are some key best practices for managing personally identifiable information:

1. Create the minimum number of privacy rules. It's difficult to analyze and maintain many privacy rules.
2. Create the strictest possible regular expressions. For example, if you want to mask a credit card number, make sure you're not masking *any* 16-digit number. Your regular expression should be as specific as possible to the data you are masking, such as:
    - Start with a new word
    - End a word
    - Have specific delimiters
    - Have specific numbers in particular positions

Regular expression examples

Here are examples of some common regular expressions:

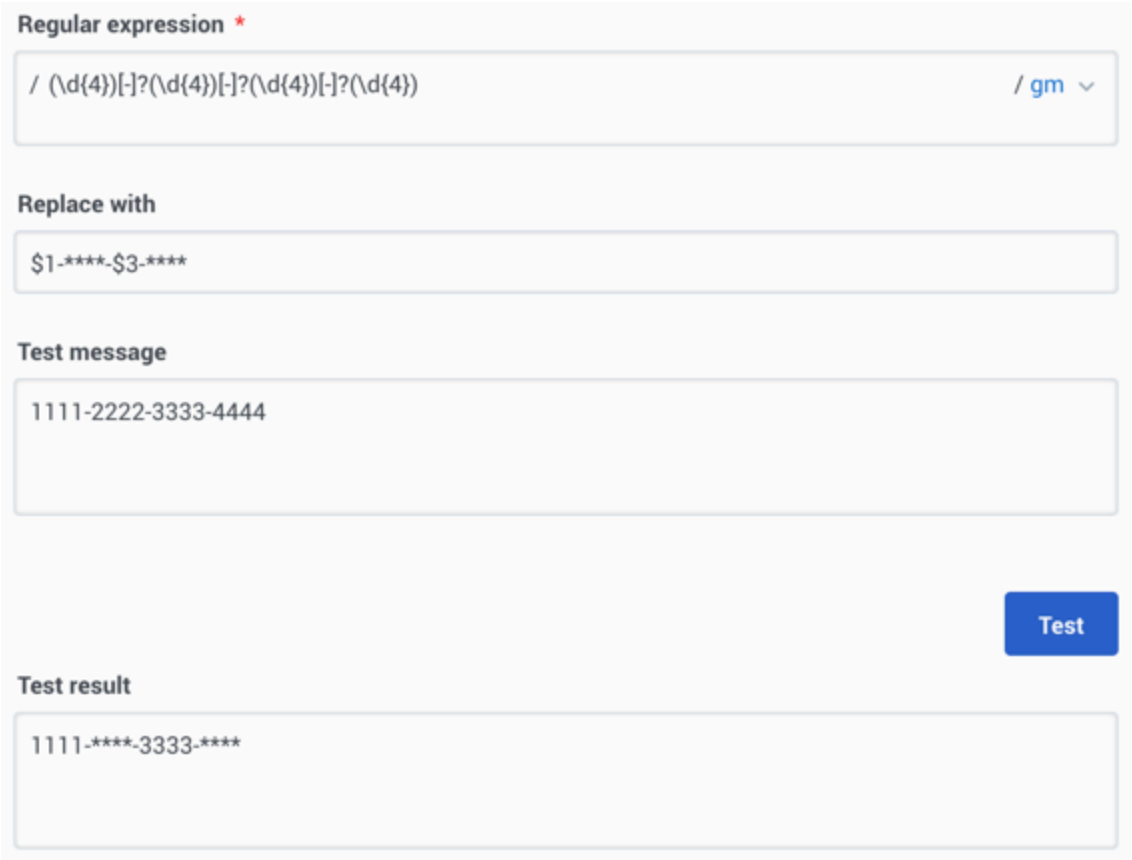
Credit Card (Visa and MasterCard only)

```
(?:^|(?]))(?:4\d{3}|5[1-5]\d{2}|6011|622[1-9]|64[4-9]\d|65\d{2})[ -.=\n\r]{0,10}\d{4}[ -.=\n\
r]{0,10}\d{4}[ -.=\n\r]{0,10}\d{4}(?:$|(?=[\Da-zA-Z(),.:;?!"'`
```

SSN (Social Security Number - U.S. only)

```
(?:^|(?]))(?!000|666|9)\d{3}[ -.=\n\r]{0,10}(?!00)\d{2}[ -.=\n\r]{0,10}(?!0000)\d{4}(?:$|
(?=[\Da-zA-Z(),.:;?!"'`
```

Partial masking



You can partially mask sensitive information by using capturing groups in your regex. Use $ in the **Replace with** field for any group you want to exclude from the mask.

To exclude more than one capturing group, each subsequent group must have at least one replacement symbol before the group in the **Replace with** field.