5.8

Bright Pattern Documentation

Generated: 7/06/2022 5:00 am

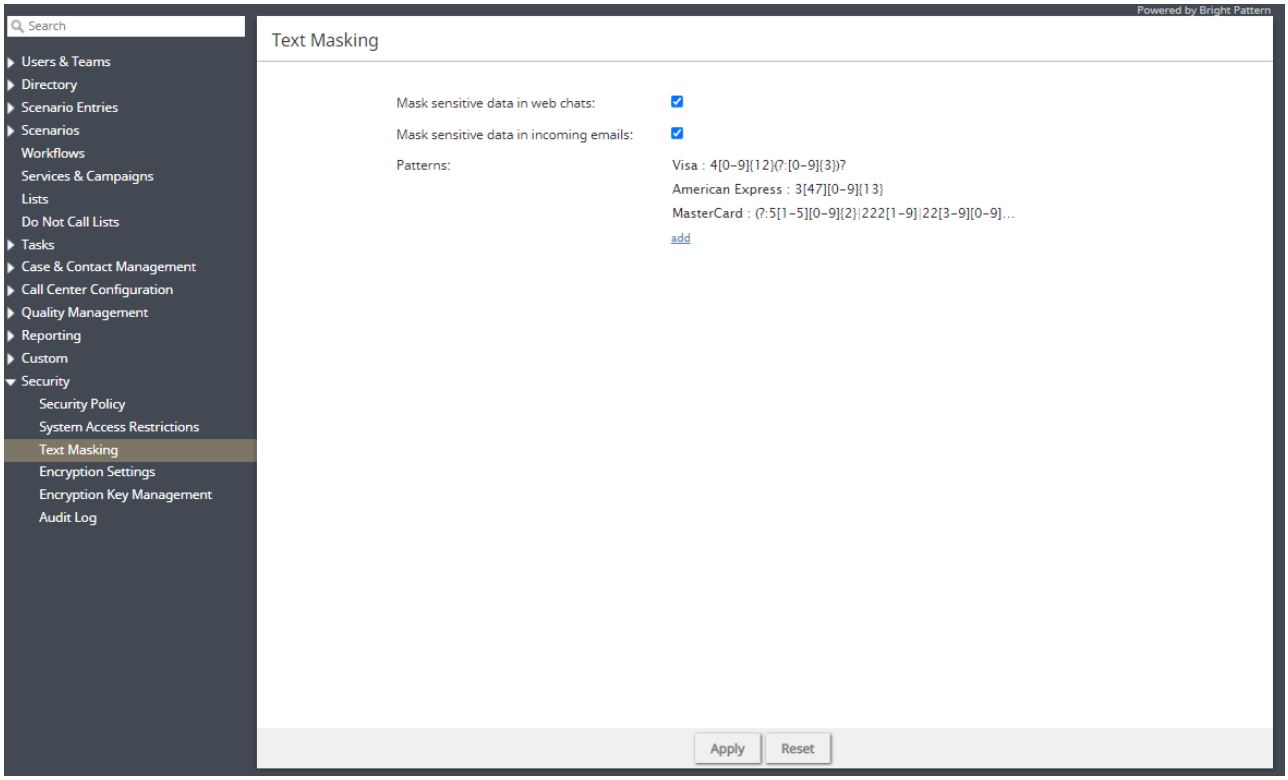
Table of Contents

Table of Contents 2
Text Masking 3
Properties 3
Mask sensitive data in web chat 3
Mask sensitive data in incoming emails 3
Patterns 4
Example Masks 4

Text Masking

Depending on the type of services that your contact center provides, incoming chats or emails may contain some sensitive data that could pose Internet security risks. Examples of such data include payment card numbers, access codes, social security numbers, and clients' personal health information. The handling of such data may be governed by various laws, industry security standards, as well as internal policies of your organization, which may require that sensitive data be masked. (Data masking is the process of hiding original data by replacing it with random characters.)

Masking can be done manually by the agents reviewing the incoming interactions and/or automatically where the system checks incoming data against some preconfigured data patterns. This article explains how to configure automatic masking. For manual data masking, see the *Agent Guide*, section *How to Remove Sensitive Data from Emails*.



Security > Text Masking

Properties

Mask sensitive data in web chat

When enabled, this setting automatically masks the text of any incoming chats that match the regex defined in Patterns.

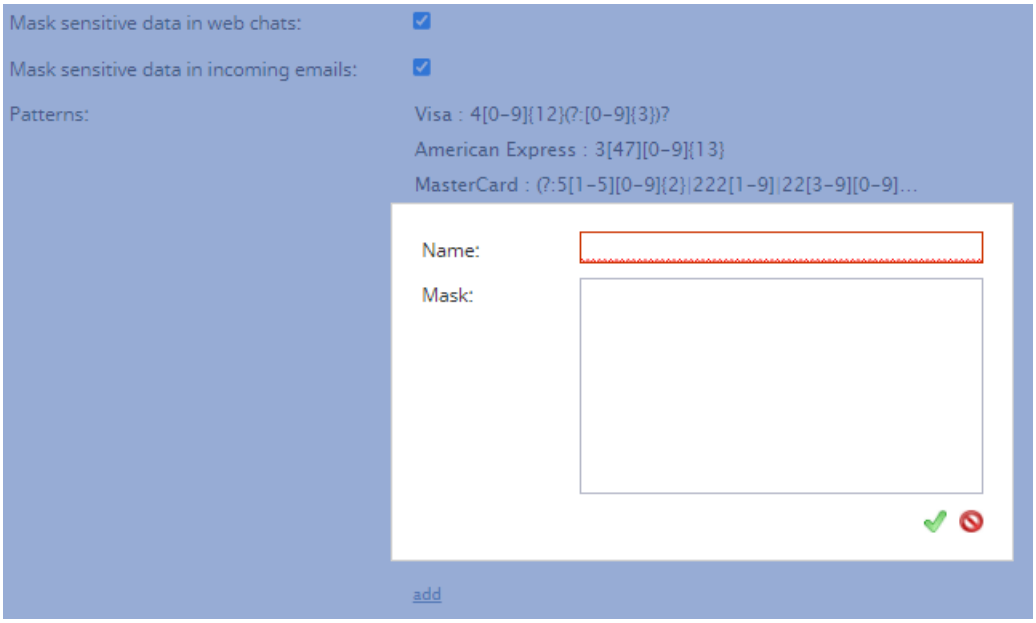
Mask sensitive data in incoming emails

When enabled, this setting automatically masks the text of any incoming emails that match the regex defined in Patterns. Note that both text and HTML versions of email bodies will be scanned and masked.

Patterns

The *Patterns* property is where you define incoming chat and email regex masks. To define a mask, click **add** to add the following values.

- **Name** - The name of your mask (e.g., "SSN")
- **Mask** - The string of values that will identify the contents of the sensitive data and replace it with a string of asterisks (i.e., **********)



Select a box to mask sensitive data

Example Masks

Masks require regex syntax. After entering an expression, click **Apply** to save your changes. Saving masks will cause any matching data element in chat and/or email messages to be "masked" in subsequent chats on the Agent Desktop application.

Note: Each expression must be entered separately.

Credit card masking:

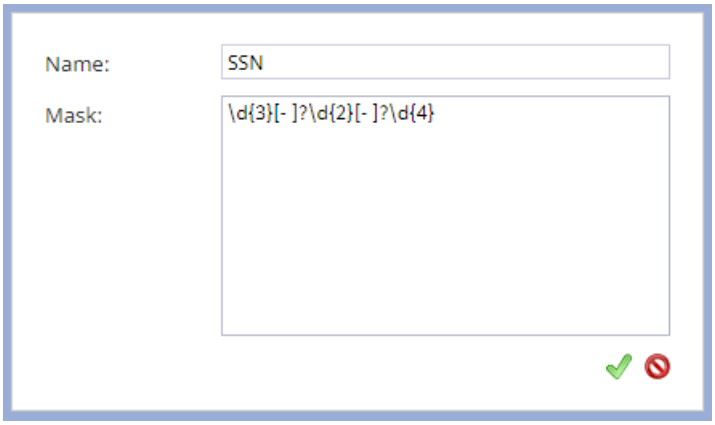
- Visa: 4[0-9]{3}[-]*[0-9]{4}[-]*[0-9]{4}[-]*[0-9]{4}
- American Express (Amex): 3[0-9 -]{13,18}
- MasterCard (MC): 5[1-5][0-9]{2}[-]*[0-9]{4}[-]*[0-9]{4}[-]*[0-9]{4}
- Diner's Club: 3(?:0[0-5]|[68][0-9])[0-9]{11}
- Discover:
  - 65[4-9][0-9][-]*[0-9]{4}[-]*[0-9]{4}[-]*[0-9]{4}
  - 64[4-9][0-9][-]*[0-9]{4}[-]*[0-9]{4}[-]*[0-9]{4}
  - 6011[-]*[0-9]{4}[-]*[0-9]{4}[-]*[0-9]{4}
  - 6221[-]*2[6-9][0-9]{2}[-]*[0-9]{4}[-]*[0-9]{4}
  - 6221[-]*[3-9][0-9]{3}[-]*[0-9]{4}[-]*[0-9]{4}
  - 622[2-8][-]*[0-9]{4}[-]*[0-9]{4}[-]*[0-9]{4}

- 6229[-]*[01][0-9]{3}[-]*[0-9]{4}[-]*[0-9]{4}
- 6229[-]*2[0-5][0-9]{2}[-]*[0-9]{4}[-]*[0-9]{4}

These masks will hide credit card numbers that are provided by customers in incoming chats. Note that the name (Visa, Amex, MC, etc.) of each mask does not affect the mask settings.

Social security number masking:

- \d{3}[-]?\d{2}[-]?\d{4}



Use text masking to hide Social Security numbers

This mask will hide Social Security numbers that may be provided by customers in incoming chats.