5.3 Security Overview

Bright Pattern Documentation

Generated: 12/01/2021 12:00 pm

Content is available under license unless otherwise noted.

Table of Contents

Security Policy

Your system can be configured for automatic lock out of a user account after a number of unsuccessful login attempts. An account locked-out in this manner can be subsequently unlocked either manually or automatically after a configured timeout.

You can also configure the system to force your users to change their passwords after a specified number of days, prevent them from submitting previously used passwords, and automatically disable inactive accounts.

Note that your service provider may also impose some password complexity rules, such as minimum password length, mandatory use of various character groups, and exclusion of weak passwords (e.g., usernames). If any such rules are imposed, you cannot change them. You should get descriptions of these rules from your service provider and inform your personnel about them.

To configure security policy settings, select the **Security Policy** option from the *Security* menu.

Security > Security Policy

Screen Properties

The *Security Policy* screen properties are described as follows.

Enable lockouts

Checking this box indicates that the account lockout option is enabled.

To comply with the PCI DSS security standard, this option shall be enabled.

Maximum login attempts

This property specifies the number of consecutive unsuccessful login attempts after which the account will be locked out.

To comply with the PCI DSS security standard, set this parameter to at least six attempts.

Reset attempt count after

This property specifies the amount of time after which the counter of unsuccessful login attempts will be reset.

Lockout duration

Lockout duration is the amount of time after which a locked-out account will be unlocked automatically. To disable auto-unlocking, set this parameter to “0” (zero), in which case, locked-out accounts can be unlocked manually only.

To comply with the PCI DSS security standard, set this parameter to at least 30 minutes.

Password history

The *Password history* section allows you to prevent the user from submitting a new password that is the same as any of the specified number of previous passwords that the user used.

Check against previously used passwords

To comply with the PCI DSS security standard, select the checkbox for*Check against previously used passwords*.

Number of previously used passwords to keep

To comply with the PCI DSS security standard, set the number to 4 (or greater).

Expiration policy

The *Expiration policy* section provides control over how often users will be required to change their passwords and after how many days inactive user accounts will be disabled.

Require users to change passwords every

This parameter allows you to specify how often users will be required to change their passwords. To comply with the PCI DSS security standard, set this parameter to no more than 90 days.

Disable inactive accounts after

This parameter allows you to specify after how many days inactive user accounts will be disabled; an inactive account is defined as an account not currently in use. To comply with the PCI DSS security standard, set this parameter to no more than 90 days.

System Access Restrictions

The system may be configured to limit access from a number of predefined IP address ranges.

To configure such IP address ranges, go to *Security* > *System Access Restrictions*.

Security > System Access Restrictions

Limit system access by client IP address

Select this checkbox to enable IP address verification.

When enabling *Limit system access by client IP address*, you can define addresses for each subsection. Note that the default setting is *<Any>* in the Agent Desktop and Contact Center Applications section and the "Privileged Access IP Range" section, which means there is no limiting. Once IP addresses are defined in these sections, *<Any>* will disappear.

Defining IP Address Ranges

You can define the range of IP addresses for the Agent Desktop and Contact Center Administrator applications, for privileged users (i.e. , and, if necessary, for access via APIs by clicking **add** in the following sections as appropriate:

- **Allow Agent Desktop and Contact Center Administrator applications access from following IP address ranges** - Allows access to these Bright Pattern applications from defined IP addresses; the default setting is *<Any>*
- **Allow users with "Privileged Access IP Range" privilege from following address ranges**- Allows users (e.g., administrators) to be able to log in to the system from a defined IP address (e.g., a public place such as a coffee shop); the default setting is *<Any>*
- **Allow API access from following IP address ranges**- Allows access via APIs

The desired IP address range should be expressed as a combination of the base IP address and a mask. The mask is used to define which bits in the base IP address are fixed and which bits are variable. A 1 bit is used to indicate a bit in the IP address that is fixed, while a 0 bit indicates that the bit is variable. Use variable bits will form the desired range.

Example Usage

If you set the following, System Access Restrictions will be from address 192.168.64.0 to address 192.168.64.63.

- **Address:** 192.168.64.63
- **Mask:** 255.255.255.192

If you set the following, System Access Restrictions will be from address 192.168.64.128 to address 192.168.64.192.

- **Address:** 192.168.64.128
- **Mask:** 255.255.255.192

Text Masking

Depending on the type of services that your contact center provides, incoming chats 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. Thus, while reviewing incoming mail, you may be expected to identify such data and make sure it is masked before the email is further processed and stored. (Data masking is the process of hiding original data by replacing it with random characters.)

It is possible to mask sensitive data not only in emails, but also in chats. To mask a fragment of an incoming chat, you must first set up the functionality in the Contact Center Administrator application in *Configuration* > *Security* > *Text Masking*.

Properties

In the properties pane that appears, check the box for **Mask sensitive data in web chat**. This enables text masking. Then click **add** to add values.

- **Name** - The name of your mask (anything you like)

- **Mask** - The string of values that will identify the contents of the sensitive data and replace it with a string of asterisks (i.e., ****************) Check the 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 such sensitive data in chats to be "masked" in subsequent chats on the Agent Desktop application. Masking sensitive data ensures that when the chat conversation is saved, or when the chat transcript is provided to the customer or other users via email, the customer's confidential personal information is hidden.

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.

Text Masking can be used to hide credit card numbers, as shown in this example

Social security number masking:

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

Use text masking to hide Social Security numbers

This mask will hide a Social Security number that may be provided by customers in incoming chats. Note that the name of the mask does not affect the mask setting.

Encryption Settings

Recordings and transcripts of all your contact center interactions can be encrypted while they are stored in the Bright Pattern Contact Center system.

Before you can use the encryption capability, it must be enabled for your contact center at the service provider level.

To enable encryption, go to *Security* > *Encryption Settings* and check the items that you intend to store encrypted.

Select from the following:

- Encrypt chat transcripts
- Encrypt SMS transcripts
- Encrypt stored email messages and attachments
- Encrypt screen recordings
- Encrypt voice recordings and transcripts

Security > Encryption

When you export any encrypted items out of the system, they will be unencrypted for export.

For more information about the method and keys used for encryption, see section Encryption Key Management.

Encryption Key Management

Bright Pattern Contact Center supports optional encryption for various data elements that are stored in the system and may contain sensitive information about your customers. This includes voice and screen recordings, chat and SMS transcripts, and email texts and attachments. For more information about enabling encryption for these data elements, see section Encryption. Custom fields of calling lists and activity forms can also be encrypted. For more information, see section Lists of this guide and section Field of the *Bright Pattern Contact Center Form Builder Reference Guide*, respectively.

Before you can use the encryption capability, it must be enabled for your contact center at the service-provider level. When this capability is enabled, a data encryption key will be generated automatically by the system. You can manually generate a new encryption key at any time. To generate a new data encryption key, select the **Encryption Key Management** option from the *Security* menu and click the **Generate a new encryption key** button.

Security > Encryption Key Management

Old encryption keys are stored in the system; they are used to decrypt the data that was encrypted using those keys. You can view the date and time of generation of the current and previous keys.

Note that in compliance with various data security standards, data encryption keys themselves are encrypted with a key encryption key (KEK), which is stored separately.

The AES-256 algorithm is used for encryption of both the data and encryption keys.

When you export any encrypted items out of the system, they will be unencrypted for export.

Audit Log

Bright Pattern Contact Center keeps track of all changes applied to the contact center configuration by all users. You can view information about these changes using the audit log function. The audit log also includes information about every attempt to log into the Contact Center Administrator application as well as every instance of access to voice and screen recordings.

Note, that in order to view the audit log, you must be assigned a role that has the *View Audit Log* privilege. By default, only the *Service Administrator* and *System Administrator* roles have this privilege.

To view the log, select **Audit Log** option from the *Security* menu. The upper area of the application pane will display various filter options that you can use to define your search criteria.

Security > Audit Log

Filters

The *Audit Log* filters are described as follows.

From/To

The *From/To* filter returns records about the operations that happened within the specified time interval. Leave the **To** field blank if you want to get all records up until the present moment.

Who

The *Who* filter returns records about the operations performed by the specified user.

Item

The *Item* filter returns records about the operations applied to the resource with the specified name. This filter should normally be used in combination with filter *Type*.

Operation

The *Operation* filter returns records about the operations of a particular type (i.e., add, delete, update, etc.).

Type

The *Type* filter returns records about the operations with the resources of a particular type (i.e., service, user, etc.)

Screen

The *Screen* filter returns records about the operations with resource properties that are defined in a particular screen. When you select the resource type using filter *Type* above, this option will display only the screens that are used to edit properties of the resources of the selected type.

Note the following:

- Clicking **Reset** will set all the filter options to their default values. The default search returns log records about all operations applied to your contact center configuration in the last seven days.
- Once the filter options are specified, click the **Filter** button to obtain the log records that meet your search criteria. The log records will be listed in the reverse chronological order. You can collapse the filter options temporarily to provide more room for viewing the results of the search.

Audit Log Data Fields

The *Audit Log* data fields give more details for each record, and they are described as follows.

Audit Log Summary

When

When gives the time stamp of the corresponding operation.

Who

Who specifies the username of the person who performed the operation.

Screen

The *Screen* is particular screen of the Contact Center Administrator application where the operation (i.e., action) was applied to a specific resource property.

Type

This is the *Type* of resource to which the operation was applied.

Summary

Summary provides details of the operation, such as the specific properties that were affected and, where applicable, the new values that were applied. If all summary information does not fit in the visible area of the table cell, you can mouse-over or click on that cell and view the entire *Summary* content in a pop-up window.

Note: You can change the order in which log records are sorted using the drop-down menu that appears when you mouse-over the corresponding column header. The same menu also allows you to disable display of any column if you need to make more room to view content of other columns.