Setting up Information Privacy
Reflection Desktop

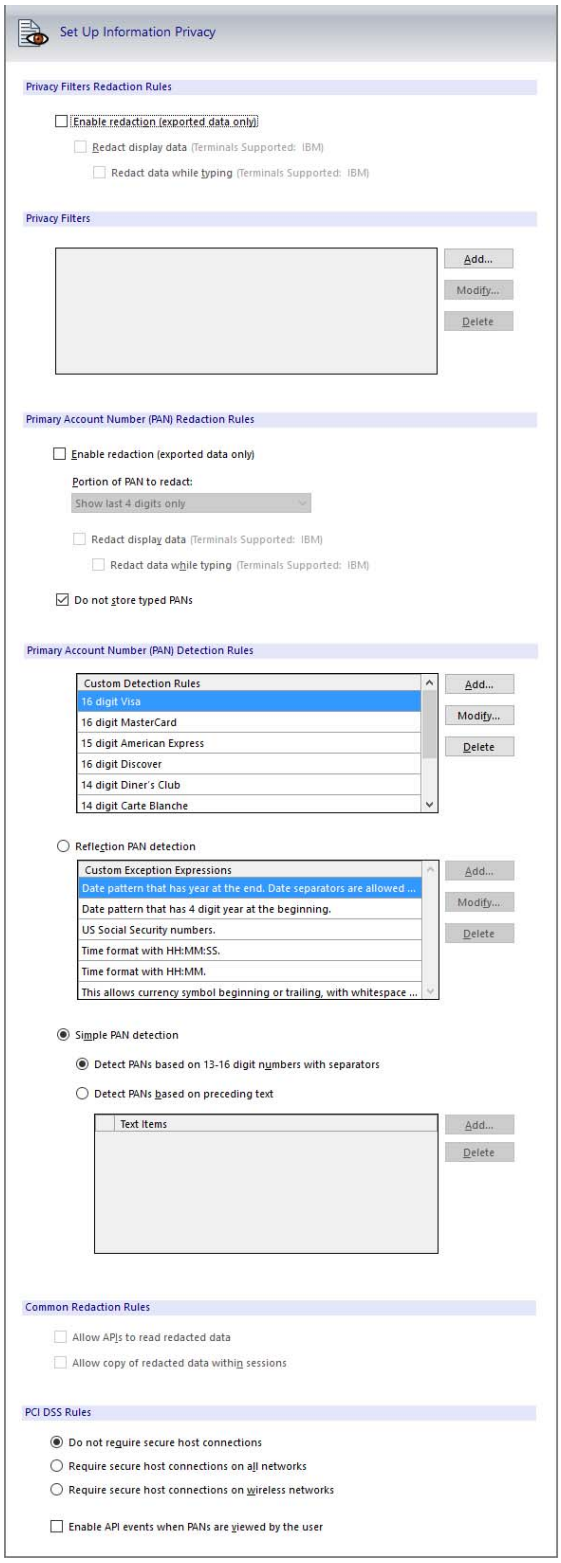
Micro Focus® Reflection®

MICRO FOCUS®

Attachmate Corporation
705 Fifth Avenue South
Seattle, WA 98105
USA
+1.206.217.7100
http://www.attachmate.com

Introduction

Reflection® Desktop products include support for several information privacy features that are designed to help you comply with industry and government regulations, like Payment Card Industry Data Security Standards (PCI DSS) that address data protection concerns. You can configure Reflection to protect sensitive data so that it is not displayed in Reflection productivity features like Screen History, and when sharing host data using Windows copy/paste for integration with other applications. For IBM hosts, you can mask sensitive data so that it is not displayed on host screens. You can also require secure connections for sessions that handle sensitive data.



This paper shows how to configure Reflection to support PCI DSS requirements.

- ☐ *PCI DSS and Reflection Desktop* on page 2 describes Reflection support for PCI DSS and provides references to relevant documentation.
- ☐ *What You Need to Do* on page 4 is a high level summary of how to configure Reflection to protect information privacy.
- ☐ *Setting up Redaction of Primary Account Numbers* (PAN) on page 5 provides in-depth information about the three Reflection options for credit card PAN (Primary Account Number also referred to as “credit card number”) detection: *Simple PAN Detection*, *Simple PAN Detection with Preceding Text*, and *Reflection PAN Detection*. This section includes suggestions about when to use each option, the considerations of each, and examples of how to set them up.
- ☐ *Setting up Privacy Filters* on page 11 includes suggestions for using simple expressions to create privacy filters that redact personal data such as phone numbers or US Social Security numbers.
- ☐ *References* on page 12 provides references to general industry PCI DSS documentation and tutorials for creating regular expressions (used for PAN identification).

PCI DSS and Reflection Desktop

What is PCI DSS?

PCI DSS (Payment Card Industry Data Security Standard) is a proprietary information security standard comprising technology requirements and process requirements designed to prevent fraud when handling credit card information. All companies who handle credit cards are subject to this standard.

To be PCI DSS compliant, organizations must meet twelve PCI DSS requirements. (Reflection aids compliance with the requirements shown in bold).

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. **Protect stored cardholder data.**
4. **Encrypt transmission of cardholder data across open, public networks.**
5. Use and regularly update antivirus software.
6. **Develop and maintain security systems and applications.**
7. **Restrict access to cardholder data by business need-to-know.**
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. **Track and monitor all access to network resources and cardholder data.**
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

How Reflection Supports PCI DSS

As shown above, Reflection supports PCI DSS requirements 3,4,6,7 And 10.

Requirement 3: Protect stored cardholder data
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). Obtain and examine written policies and examine displays of PAN (for example, on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.

You can set up PAN (Primary Account Number, also referred to as “credit card number”) redaction rules to redact PANs that appear in Reflection productivity features, like Screen History, and when sharing host data using Windows copy/paste for integration with other applications. For IBM hosts, you can also choose to redact PAN data displayed on screens, either as the PAN is typed or after it is entered.

Reflection provides several options for identifying and redacting PAN data. (See *Setting up Redaction of Primary Account Numbers* on page 5.) For more information, *see Configuring PCI DSS* in the Reflection Desktop Help.

Requirement 4. Encrypt transmission of cardholder data across open, public networks.
***4.1** Verify the use of security protocols wherever cardholder data is transmitted or received over open, public networks.*

You can configure Reflection to disallow non-secure connections on wireless networks. On the Information Privacy dialog box, under PCI DSS rules, you can require secure host connections for all network connections or for wireless only. (Secure connections are connections that are configured to use a security protocol.) See What *You Need to Do* on page 4 or *Configuring PCI DSS* in the Reflection Desktop Help.

Reflection supports security protocols such as SSH, Kerberos, and SSL, which include: secure authentication, data encryption, and validation of data integrity. See *Set up Secure Connections for Reflection* in the Reflection Desktop Deployment Guide.

***4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).*

You can set up Reflection to filter credit card data on the fly. (See What *You Need to Do* on page 4 or *Configuring PCI DSS* in the Reflection Desktop Help.)

Requirement 6. Develop and maintain security systems and applications.
Attachmate provides technical notes and downloads for security vulnerabilities. (See http://support.attachmate.com/security/).

Requirement 7. Restrict "access" to PAN based on current user identity.
PCI DSS feature behavior is based on the current user identity. You can configure different PCI DSS settings for trusted and non-trusted users, and deploy these via customized installations to different user groups as necessary. See the Reflection Desktop Deployment Guide.

Requirement 10. Track and monitor all access to network resources and cardholder data.
***10. 2.1** Verify all individual access to cardholder data is logged.*
In many cases a security breach can be mitigated more efficiently if the organization knows which information leaked. Reflection includes an advanced .NET application programming interface (API) for programmatic access to the Reflection features. The .NET API and VBA *CreditCardRecognized* event can be set to fire whenever a credit card is displayed or copied. You can handle this event to create logs or perform other actions required for compliance. (See What *You Need to Do* on page 4, the .NET API Guide, or the VBA Guide for an example of how to handle an event to log access to cardholder data.)

Note: This event is fired only if the credit card is seen in its entirety (e.g. “in the clear”). It does not fire if a user is able to see only redacted PANs.

What You Need to Do

To set up Reflection to protect sensitive data, you’ll need to configure the following options in the Information Privacy Dialog Box:

1. Under Primary account PAN Number Redaction Rules, choose **Enable Redaction** and then select options for displaying redacted data. If you want to prevent PAN data from being saved in an external file, end user messaging devices, or any component that saves screen data, such as the Reflection Recent Typing feature, select **Do not store typed PANs**.

   Note: “Redact display data” and “Redact data while typing” options for both privacy filters and PAN detection currently apply only to IBM emulation sessions. They are not currently implemented for VT.

2. Set up Primary Account Number (PAN) Detection Rules. You will need to choose a redaction method and configure it as shown in *Setting up Redaction of Primary Account Numbers* on page 5.
3. If you want to use Privacy Filters, you will need to configure the Privacy Filter Redaction Rules and then create a simple or regular expression for the filter as shown in *Setting up Privacy Filters* on page 11.
4. Under PCI DSS Rules, set up requirements for secure connections. You can require secure connections for all network connections or for wireless only. (*See Configuring PCI DSS* in the Reflection Desktop Help.)
5. If you want to log access to credit card data, select **Enable API events when PANs are viewed by the user**. Then follow the instructions in the NET API Guide or the VBA Guide for an example of how to handle an event to log access to cardholder data.

Setting up Redaction of Primary Account Numbers

You can choose from three methods for redacting credit card PAN data: Simple Primary PAN Detection, Simple PAN Detection with Preceding Text, or Reflection PAN Detection.

Method	Use when…	Considerations
Simple PAN Detection matches a credit card number sequence.	All of the credit card data in your host applications are displayed and entered in a “contiguous” fashion. You are only detecting PANs for the prepackaged major credit card issuers.	Easy to set up
Simple PAN Detection with Preceding Text matches preceding text (e.g., *Account*) followed by a credit card number sequence.	Same as above except credit card data in your host applications are always labeled in predictable ways.	Relatively easy to set up Avoids false positives
Reflection PAN Detection uses regular expressions to detect PANs.	You need to define custom card issuer patterns to detect, such as oil company or department store cards. PANs appear in a non-contiguous format or are entered using non-standard digit group separators. You want PAN detection to be especially “aggressive” or “greedy” in that any digit grouping on any screen should be considered for redaction, and you need to be able to redact without regard to what other text or digit separators may appear between single or groups of digits in the PAN.	Allows the greatest degree of flexibility and customization for unique detection needs omputationally-intensive— can degrade performance on PCs with limited processing power or memory The likelihood of “false positive” redaction is much greater with this method than the other two, especially if your host screens are very digit-laden

Setting up and using Simple PAN Detection

When Simple PAN Detection is selected, Reflection matches a credit card number sequence (a 13-16 digit number).

Note: The credit card character sequences can also include whitespace and hyphen characters as digit grouping separators.

When to use Simple PAN Detection

Use Simple PAN Detection when your application meets all of the following conditions:

☑ All of the credit card account numbers in your host applications are displayed and entered in a "contiguous" fashion. In other words, the PANs always appear or are always entered as a single continuous string (e.g. 1111-1111-1111-1111, 2222 2222 2222 2222, 444444444444444 etc.).

☑ All of the account numbers that need to be redacted are from one or more of the following issuers: Visa, MasterCard, American Express, Discover, Diner's Club, Carte Blanche, Voyager, JCB, or enRoute.

If data in your application are displayed or entered in a noncontiguous fashion or you need to detect other card issuers, use the Reflection PAN Detection option and enter additional custom patterns for those issuers in the Custom Detection Rules table, or use privacy filters to specify a custom pattern.

Advantages of Simple PAN Detection

This method requires no additional configuration and should be suitable for most situations.

Considerations for Simple PAN Detection

Although simple PAN Detection is easy to set up and use, there are a few items to consider when using this method:

- This method works only with the major credit card issuers noted above. (In some cases, privacy filters can be used in conjunction with this method to add additional issuers.)
- It is possible to get false positives in entry fields where large numbers of digits are entered consecutively and where there are no non-digit separator characters delimiting the overall sequence of digits.

How to set up Simple PAN Detection

On the Information Privacy dialog box, select Enable Redaction and then select Simple Redaction.

Setting up and Using Simple PAN Detection with Preceding Text

When Simple PAN Detection is selected, Reflection matches preceding text (e.g., keywords like "Account") followed by a credit card number sequence (a 13-16 digit number).

EG: The credit card character sequences can also include whitespace and hyphen characters as digit grouping separators.

When to use Simple PAN Detection with Preceding Text

Use Simple PAN Detection with Preceding Text when your application meets all of the following conditions:

☑ All of the credit card account numbers in your host applications are displayed and entered in a "contiguous" fashion. In other words, the PANs always appear or are always entered as a single continuous string (e.g. 1111-1111-1111-1111, 2222 2222 2222 2222, 444444444444444 etc.).

☑ All of the account numbers that need to be redacted are from one or more of the following issuers: Visa, MasterCard, American Express, Discover, Diner's Club, Carte Blanche, Voyager, JCB, or enRoute.

☑ Your host application screens that contain credit cards are very well defined, and credit card information is always "tagged" or prefixed in predictable ways. For instance, your host application has only a handful of screens that contain (or potentially can contain) credit card numbers, and those numbers on the screen are always preceded by a label such as "Account Number: "or "Credit Card."

Advantages of Simple PAN Detection with Preceding Text

Simple PAN Detection with Preceding Text has the following advantages:

- This method further restricts the data subject to potential redaction and can serve to virtually eliminate “false positives” in other areas of the screen that do not contain credit card data.
- Any potential card number, even valid ones, are not considered unless they immediately follow one of the defined strings and the digits do not contain any other data but digits, whitespace, and hyphen separators. This is appropriate for screens/host applications that contain a lot of other numeric data that should not be considered for redaction.
- If your host applications have a large numbers of “digit intensive” screens, especially ones that contain lengthy digit data such as part/SKU numbers, ISBN numbers, etc., use of this option greatly reduces the chance of accidental “false positives” in data that could mistakenly be detected as a credit card number.

Considerations for Simple PAN Detection with Preceding Text

Simple PAN Detection with Preceding Text has a few items to consider when using this method:

- Before you deploy Reflection, you will need to define the text strings that precede card numbers. This means examining your host applications and noting the strings that precede areas where credit cards are either displayed (protected) or entered (unprotected).
- Redaction occurs only after defined text strings. The entire PAN must appear immediately after one of the defined strings, without any additional non-digit, non-whitespace/hyphen separator characters appearing.
- This method cannot detect credit cards that use separator text or characters (other than whitespace or hyphens) that are mixed in with the full account number (e.g. “1111 / 3333 / 4444 / 5555”, “first: 1111 second: 2222 third: 3333 fourth: 4444”).

How to set up Simple PAN Detection with Preceding Text

1. In your host application screens, identify all of the keywords that precede credit card numbers.
2. On the Information Privacy dialog box, select **Enable Redaction** and then select **Simple Redaction**.
3. In the Information Privacy dialog box, select **Detect PANs based on preceding text** and add the keywords to the “Text Items” table.

Setting up and Using Reflection PAN Detection

When Reflection PAN Detection is selected, Reflection uses the following process to detect credit card PAN data:

1. Read a host screen’s data as input.
2. Mask out “exclusion patterns” of digit data that are defined as “not credit card data.”
3. Remove all non-digit data from the input host screen data (leaving just a continuous ordered string of digits).
4. Apply recognition methods to the remaining digit-only data using stock credit card patterns (provided with Reflection) and specified custom credit card patterns of 13 to 16 digits, from left to right.

5. Redact recognized PANs within this data.

Note: Only matches that pass checksum calculation according to the Luhn Algorithm are redacted.
(The Luhn Algorithm, also known as the "modulus 10" or "mod 10" Algorithm, is a checksum formula used to identify identification numbers (see http://en.wikipedia.org/wiki/Luhn_algorithm).

6. Merge any redactions back into the original host screen data.
7. Restore the data that was masked by exclusion patterns.

You can specify custom credit card patterns that you want Reflection to recognize. To avoid “false positive” redaction, you will also likely need to define additional exclusion patterns (or literal strings containing digits such as application ids, screen ids, or copyright notices).

When to use Reflection PAN Detection

Use Reflection PAN Detection for any of the following applications:

☑ You need to detect non-standard credit card patterns/issuers (for instance, oil company or department store cards).

☑ Your host application has specialized screens where credit cards can be entered or are displayed in non-standard ways (e.g., non-contiguous sets of digits such as multiple input fields of data arranged in a vertical table or contiguous sets of digits using nonstandard digit group separators).

☑ You want PAN detection to be especially “aggressive” or “greedy” in that any digit grouping on any screen should be considered for redaction, and you need to be able to redact without regard to what other text or digit separators may appear between single or groups of digits in the PAN.

Advantages of Reflection PAN Detection

Reflection PAN Detection allows the greatest degree of flexibility and customization for unique detection needs:

- This method can be configured to detect non-standard credit card issuer patterns of 13-16 digits.
- If you have host application screens with other numeric data such as part or SKU numbers that look very similar to credit cards, you can exclude those custom patterns from redaction.
- This method can detect credit cards that use separator text or characters (other than whitespace or hyphens) that are mixed in with the full account number (e.g. “1111 / 3333 / 4444 / 5555”, “first: 1111 second: 2222 third: 3333 fourth: 4444”).
- This method is suitable for applications that have host screens where credit cards are entered in multiple fields, especially if the screens are laid out in a vertical “table” format.
- This method allows detection and redaction of PANs that have nonstandard digit group separation or other random string data in between the digits.

  For example, the following input data can be detected as a PAN with this method, assuming 1111222233334444 is a potential valid credit card number:

  First: 1111 Second: 2222 Third: 3333 Fourth: 4444

  Or

  1111#2222#3333#4444

  The other methods could not be used to detect a credit card number that appears in such a way.

Considerations for Reflection PAN Detection

There are few items to consider when using the Reflection PAN Detection method:

- This is the most complex method to set up. In order to configure exclusion patterns, you will need to be familiar with regular expressions and their syntax.
- This method is the most computationally-intensive. It can result in performance degradation and increase response time on PCs with limited processing power and/or memory, especially when the "Redact data while typing" option is selected.
- The likelihood of "false positive" redaction is much greater with this method than the other two, especially if your host screens are very digit-laden.
- It is likely that you will need to go through a review process with all of your host applications to eliminate false positives, by identifying and defining exclusion patterns that are not supported "out of the box". Some examples of these are custom part or SKU numbers for inventory applications, screen or application numeric identifiers, copyrights, international phone number formats, and the like.

How to Set up Detection Rules

To set up detection rules, you specify the custom credit card sequences (patterns) that you need Reflection to recognize.

To enter a custom credit card number sequence, add a regular expression that specifies the pattern the sequence must follow to the Custom Detection Rules table. Because the Reflection PAN Detection method detects digit-only data, do *not* enter digit grouping separator characters such as hyphens or whitespace in these custom expressions.

IMPORTANT: These patterns are applied on "remaining digit" data only, i.e. a string of all digits on the screen that have not been excluded by stock or custom exclusion patterns. Therefore, the custom PAN pattern should *not* include non-numeric data such as separators, nor can it contain specifications of preceding or trailing characters, whitespace, or word boundaries.

To match fixed prefixes, you can combine literal text with a regular expression. Typically card issuers have a prefix of 1 or more digits that are fixed, followed by the remainder of digits that can vary. If the prefix is always "static" this can be expressed with literal text in the regular expression. Do *not* specify something like `\d{16}`, which would match *any* 16 digit number. An expression like this is very likely to result in unintended false positives!

Examples of regular expressions that detect credit card PANs

Example 1: Using a regular expression

To detect cards issued by a fictitious *Acme Corporation*, which are always 15 digits starting with "7200", you might add the following regular expression:

```
7200\d{11}
```

This means match all consecutive instances starting with "7200" followed by any 11 additional digits.

E*xample 2: Using literal text and a regular expression*

Let's say we need to detect cards issued by a fictitious "National Bank" that are 16 digits starting with "88" with the next digit ranging from 0 to 5 (e.g. 880, 881, 882, 883, 884, or 885 are the valid prefixes). One could add the following regular expression for this case:

```
88[0-5]\d{13}
```

This is read as "match the literal text `88`, followed by a digit in the range `0-5` inclusive, and followed by 13 additional digits.

How to Set up Custom Exclusions to avoid false positives

Because Reflection PAN Detection disregards the context of non-digit text when detecting PANs, all digits appearing on the screen could potentially be aggregated together to form a potential PAN. It is likely that your host screen data contains digit data that is not to be considered for PAN redaction.

To exclude this data from PAN redaction, Reflection uses a set of regular expressions. These exception expressions are listed in the Custom Exception Expressions table, in the Information Privacy dialog box. Reflection provides exception expressions that exclude some common digit patterns, such as North American phone numbers, currencies, short date/time formats, US social security numbers, and others.

However, you can also exclude digit formats that are proprietary to your applications, such as custom screen identifiers or inventory part/SKU numbers. To exclude proprietary formats from the redaction process, you will need to add one or more regular expressions to the Custom Exception Expressions table. Literal strings (such as screen ids, copyright notices/dates, etc.) can also be specified here.

IMPORTANT: Unlike the expressions that detect credit card PANs, the expressions for exclusions are applied to the input screen data before removal of non-digit data. These expressions should be specified "as they would appear" on the original host screen.

Examples of Custom Exclusions

Example 1: Using a regular expression

In the USA, postal (or ZIP) codes can follow two formats – 5 consecutive digits, or 5 consecutive digits followed by a hyphen and four additional digits. Typically, on a host application information screen, these codes are preceded and trailed by at least one space character. If we had a screen like this we could add the following expression to the Custom Exception Expression table to eliminate one potential source of "false positives" by excluding ZIP codes from redaction:

```
\s\d{5}([\-]\d{4})?\s
```

When we read this expression from left to right, it says "match a leading whitespace character, followed by 5 consecutive digits, and then match zero or one instance of a character group consisting of one hyphen followed by 4 additional digits, followed by a whitespace character."

Note: Regular expression syntax sometimes requires the "escaping" of certain reserved characters. In this case, the hyphen must be escaped since it is specified within a character group (the text within the parentheses enclosed in square brackets above).

This expression would match strings like " `88888` ", " `88888-7777` ". Because leading and trailing whitespace is required, strings like "`88888`" and "`88888-7777`" would NOT be matched. Omitting the \s in the expression above would result in matches where the digit patterns are embedded inside other longer strings.

For instance if the expression were modified to:

```
\d{5}([\-]\d{4})?
```

Unlike when we included the \s in the expression, the following text strings would result in a match:

```
Foo88888Bar
Embedded88888-7777Text
Prefix88888
88888-7777Suffix
```

Example 2: Using an exact literal string:
Some of the host screens in an application have a copyright date string such as “Copyright © Acme Corporation 1990, 1992, 2004” that could cause a false positive. In this example, we will exclude the digits in that string from PAN redaction processing.

This can be solved by entering the exact literal string that is desired for exclusion. In this case enter this string in the exclusion expression table:

```
Copyright © Acme Corporation 1990, 1992, 2004
```

IMPORTANT: When developing custom regular expressions, it is highly recommended to use a regular expression development and test tool to ensure that the expression truly behaves as you intended. In other words, it matches ONLY what you intend to match and does not match text that you don’t want. One such freeware tool is the Expresso regular expression development tool that can currently be found at http://www.ultrapico.com/Expresso.htm. This tool requires registration to use beyond an introductory trial period, but is currently free to use upon completion of registration.

Also, there are many common patterns that have regular expression implementations “published” in the public domain. An internet search for “regular expression library” will turn up several sites that can be searched for pre-constructed regular expressions. One popular site is http://www.regexlib.com. These can be used as a starting point for your own expressions.

Make sure that you thoroughly test expressions before they are deployed for Reflection.

Setting up Privacy Filters

You can set up privacy filters to protect personal information that is not credit card data. You can also use these filters together with the Information Privacy redaction to enhance protection of credit card data.

Use Privacy Filters when…

Privacy filters are useful when you need to meet one or more of the following requirements:

- ☑ You have certain patterns of data outside the realm of credit card formats that you would like to redact. For instance, you may need to redact US Social Security numbers, proprietary sensitive account numbers, motor vehicle registration or license identifiers, and the like.
- ☑ You need to specify credit card patterns that fall outside the range of 13-16 digit lengths. (You could use this approach along with any of the PAN detection methods.)
- ☑ You need to specify 13-16 digit custom formats when using a PAN detection method other than “Reflection PAN Detection.”

IMPORTANT: If used in conjunction with the simple detection method based on preceding text, privacy filters do not honor the preceding text requirement.

Note: When privacy filters detect a match, ALL of the non-whitespace characters are redacted. This differs slightly from PAN redaction, where only certain portions of the PAN are redacted according to the configuration setting “portion of PAN to redact”.

You can use regular or simple expressions to set up privacy filters. Privacy filters that use simple expressions are flexible and are easy to set up: The patterns can be any combination of alphanumeric “placeholders”, wildcard specifiers (meaning they match anything) or literal text and can be set up for any length of text.

The patterns also follow a simpler syntax than regular expressions without the potentially confusing syntax and rules. The filter format should be familiar to legacy EXTRA! X-Treme customers, and is supported in Reflection 2007 and later.

IMPORTANT: Privacy Filters and PAN detection work together to keep sensitive information private. Privacy filters are applied *after* PAN detection, so keep in mind that portions of the host screen data may already be redacted by the time privacy filters are applied. This can prevent a configured filter from fully redacting data that would have "matched" had PAN redaction not been active.

To improve performance, do not duplicate existing PAN patterns in privacy filters.

How to set up Privacy Filters

In the Information Privacy dialog box, specify the Privacy Filters Redaction Rules and Privacy Filters you want to use.

References

PCI DSS Web Site

https://www.pcisecuritystandards.org/ -- Download the current PCI DSS specification here. The Reflection implementation is based on version 2.0 of the specification, issued in October of 2010.

Tools for regular expressions

The Expresso regular expression development tool that can be found at:
http://www.ultrapico.com/Expresso.htm .

This site provides common patterns for regular expressions:
http://www.regexlib.com.

Attachmate expressly disclaims any responsibility for the availability or performance of any of the tools or sources suggested in this document.