Defining Service Groups

▶ *Objects > Services Groups*

To simplify the creation of security policies, you can combine services that have the same security settings into service groups. To define new services, refer to "Defining Services" on page 152.

To define service groups, click **New** and specify the following information.

Table 73. Service Group Settings

Field	Description
Service Group Name	Enter the service group name (up to 31 characters). This name appears in the services list when defining security policies. The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.
All Services & Groups	Select the check box next to the services  and/or other service groups  to be included in this group.

About Data Patterns

Data pattern support allows you to specify categories of sensitive information that you may want to subject to filtering using data filtering security policies. For instructions on configuring data patterns, refer to "Defining Data Patterns" on page 157.

When adding a new pattern (regular expression), the following general requirements apply:

- The pattern must have string of at least 7 bytes to match. It can contain more than 7 bytes, but not fewer.
- The string match is case-sensitive, as with most regular expression engines. Looking for "confidential" is different than looking for "Confidential" or "CONFIDENTIAL."

The regular expression syntax in PAN-OS is similar to traditional regular expression engines, but every engine is unique. The following table describes the syntax supported in PAN-OS.

Table 74. Pattern Rules

Syntax	Description
.	Match any single character.
?	Match the preceding character or expression 0 or 1 time. The general expression MUST be inside a pair of parentheses. Example: (abc)?
*	Match the preceding character or expression 0 or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)*
+	Match the preceding character or regular expression 1 or more times. The general expression MUST be inside a pair of parentheses. Example: (abc)+

Table 74. Pattern Rules

Syntax	Description
|	Equivalent to "or". Example: ((bif)|(scr)|(exe)) matches "bif", "scr" or "exe". Note that the alternative substrings must be in parentheses.
-	Used to create range expressions. Example: [c-z] matches any character between c and z, inclusive.
[ ]	Match any. Example: [abz]: matches any of the characters a, b, or z.
^	Match any except. Example: [^abz] matches any character except a, b, or z.
{ }	Min/Max number of bytes. Example: {10,20} matches any string that is between 10 and 20 bytes. This must be directly in front of fixed string, and only supports ".".
\	To perform a literal match on any one of the special characters above, it MUST be escaped by preceding them with a '\' (backslash).
&amp	& is a special character, so to look for the "&" in a string you must use "&amp" instead.

Data Patterns Examples

The following are examples of valid custom patterns:

- .*((Confidential)|(CONFIDENTIAL))
  - Looks for the word "Confidential" or "CONFIDENTIAL" anywhere
  - ".*" at the beginning specifies to look anywhere in the stream
  - Does not match "confidential" (all lower case)
- .*((Proprietary &amp Confidential)|(Proprietary and Confidential))
  - Looks for either "Proprietary & Confidential" or "Proprietary and Confidential"
  - More precise than looking for "Confidential"
- .*(Press Release).*((Draft)|(DRAFT)|(draft))
  - Looks for "Press Release" followed by various forms of the word draft, which may indicate that the press release isn't ready to be sent outside the company
- .*(Trinidad)
  - Looks for a project code name, such as "Trinidad"