MarvelClient™

Zip/Unzip and Attachment Blocking

A panagenda Guide

panagenda

ZIP/UNZIP AND ATTACHMENT BLOCKING

MarvelClient 3.x

Contact

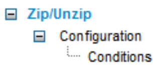
panagenda Austria
(Headquarters)
panagenda GmbH
Schreyvogelgasse 3/10
AT 1010 Vienna (Austria)
Phone: +43 1 89 012 89
Fax: +43 1 89 012 89 – 15

panagenda Germany
panagenda GmbH
Lahnstraße 17
DE 64646 Heppenheim
(Germany)
Phone: +49 6252 305 28 41
Fax: +49 6252 305 284 – 2

panagenda USA
panagenda Inc.
60 State Street
Suite 700
Boston, MA 02109 (USA)
Phone: +1 850 226 9393
Fax: +1 415 449 5940

E-Mail Sales: sales@panagenda.com
E-Mail Support: support@panagenda.com
Web: www.panagenda.com

Zip/Unzip



The *Zip/Unzip* → ***Configuration*** view in the Configuration Database lists all the Actions that are related to the configuration of MarvelClient Zip/Unzip, such as global or database specific Zip/Unzip settings.

The sub-view ***Conditions*** displays all of your existing Database Scope Conditions, if any. In all Zip/Unzip views, the action bar allows you to create Zip/Unzip related Actions and Conditions respectively.

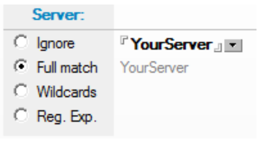
Database Scope Condition

Database Scope Conditions allow you to define a (set of) database(s), to be further associated to database specific Zip/Unzip settings.

When creating a Database Scope Condition, specify its respective *Scope* first:

- *If condition is met* = database(s) that match the Database Scope specified below in this Condition
- *If condition is NOT met* = any databases that do not match the Database Scope specified below in this Condition

The Database Scope is defined by selecting one or more of the criteria ***Server***, ***Directory***, ***Filename***, ***Replica-ID*** and ***Template name***.



Server:
○ Ignore
● Full match
○ Wildcards
○ Reg. Exp.
YourServer
YourServer

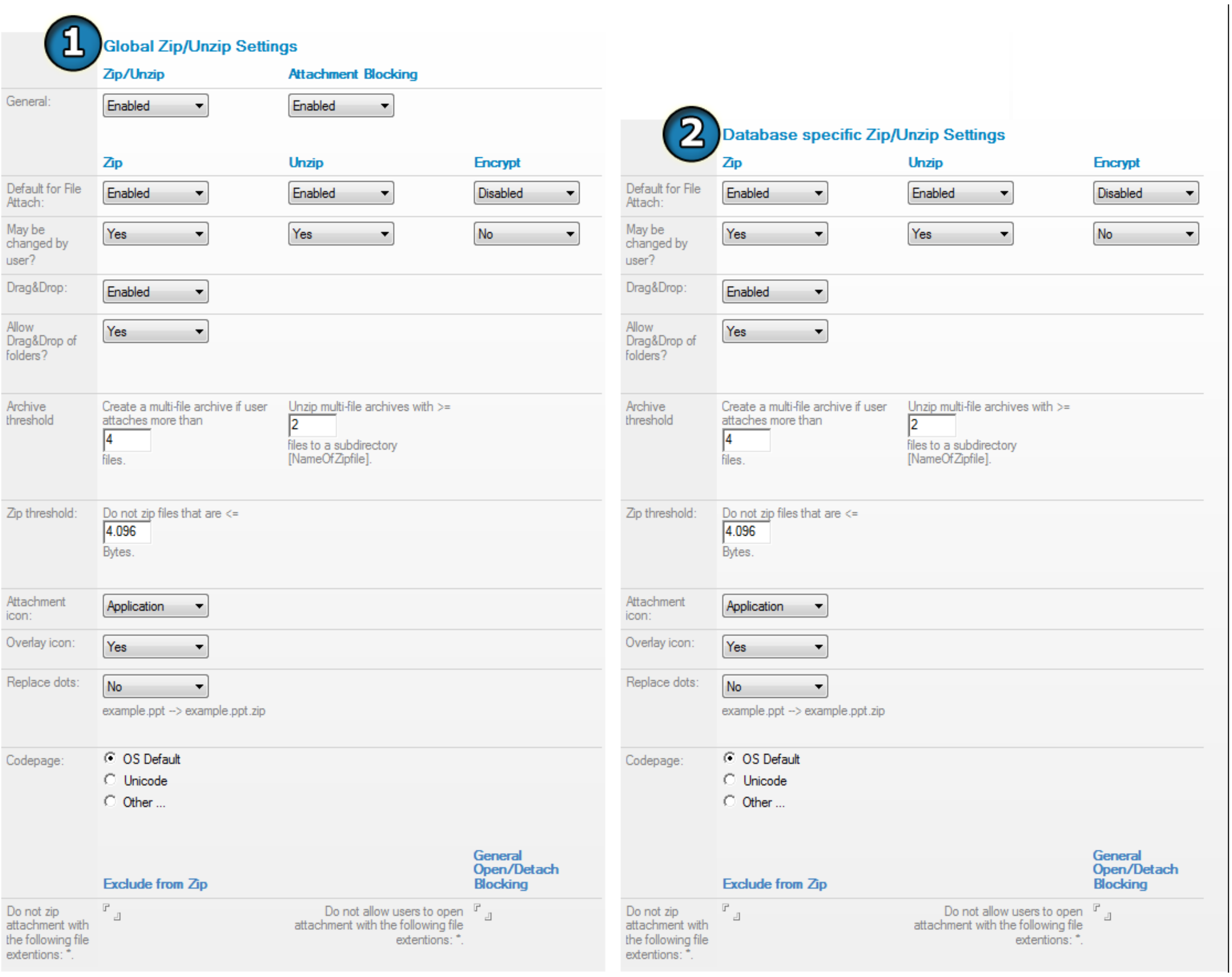
Apart from *Replica-ID*, where you only have the options *Ignore* and *Full match*, all other criteria allows you to either *Ignore* the value or perform a *Full match*, *Wildcard*, or *Reg.*[ular] *Exp.*[ression] comparison.

Wildcards allow for the use of "*" and "?", where "*" means 0-n characters, "?" means 1 character, for example:

- “**Server0?/ACME**” would match “Server01/ACME”, “Server02/ACME”, “Server0A/ ACME”, “Sever0X/ACME”, etc., but not “Server011/ACME” or “Server01A/ACME”
- “**Server0*/ACME**” however would well match all of what “Server0?/ACME” matches, as well as “Server011/ACME” and “Server 01A/ACME”

Zip/Unzip Settings (Setting Action)

The Global Zip/Unzip Settings (1) and the Database specific Zip/Unzip Settings (2) forms are quite similar:



Global Zip/Unzip Settings

	Zip/Unzip	Attachment Blocking	
General:	Enabled ▾	Enabled ▾	
	Zip	**Unzip**	**Encrypt**
Default for File Attach:	Enabled ▾	Enabled ▾	Disabled ▾
May be changed by user?	Yes ▾	Yes ▾	No ▾
Drag&Drop:	Enabled ▾		
Allow Drag&Drop of folders?	Yes ▾		
Archive threshold	Create a multi-file archive if user attaches more than 4 files.	Unzip multi-file archives with >= 2 files to a subdirectory [NameOfZipfile].	
Zip threshold:	Do not zip files that are <= 4.096 Bytes.		
Attachment icon:	Application ▾		
Overlay icon:	Yes ▾		
Replace dots:	No ▾ example.ppt --> example.ppt.zip		
Codepage:	● OS Default ○ Unicode ○ Other ...		
	Exclude from Zip		**General Open/Detach Blocking**
Do not zip attachment with the following file extentions: *.		Do not allow users to open attachment with the following file extentions: *.	

Database specific Zip/Unzip Settings

	Zip	Unzip	Encrypt
Default for File Attach:	Enabled ▾	Enabled ▾	Disabled ▾
May be changed by user?	Yes ▾	Yes ▾	No ▾
Drag&Drop:	Enabled ▾		
Allow Drag&Drop of folders?	Yes ▾		
Archive threshold	Create a multi-file archive if user attaches more than 4 files.	Unzip multi-file archives with >= 2 files to a subdirectory [NameOfZipfile].	
Zip threshold:	Do not zip files that are <= 4.096 Bytes.		
Attachment icon:	Application ▾		
Overlay icon:	Yes ▾		
Replace dots:	No ▾ example.ppt --> example.ppt.zip		
Codepage:	● OS Default ○ Unicode ○ Other ...		
	Exclude from Zip		**General Open/Detach Blocking**
Do not zip attachment with the following file extentions: *.		Do not allow users to open attachment with the following file extentions: *.	

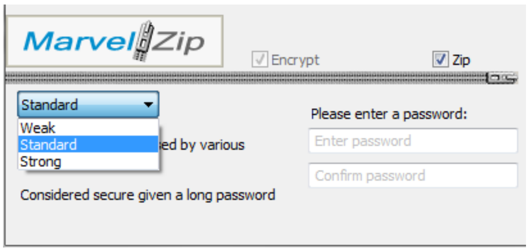
Figure 1: Zip/Unzip Settings – Global and Database Specific

Specify the settings of your choice, give the document a title and don’t forget to set up and select a **Database Scope Condition** for Database specific Zip/Unzip Settings on the *When* tab of the form – then, save the Settings document.

Details about Zip and Encryption:

The Zip/Unzip module is compatible with the de facto standard defined by PKWARE's ZIP Application Note (Version 6.3.3, see: http://www.pkware.com/documents/casestudies/APPNOTE.TXT).

The used encryption depends on the selection in the attachment file dialog:



Considered secure given a long password

Figure 2: Zip/Unzip Encryption – Attachment File Dialog

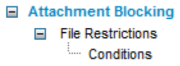
- ***Weak*** – Also known as "Standard Zip 2.0 encryption" or "Password-Protection". See Chapter 6.1 of PKZIP AppNote.txt specification (see: http://www.pkware.com/documents/casestudies/APPNOTE.TXT).
  Description in attachment file dialog: "Default password protection for old zip archives. Not recommended (unsecure)"
  - Vulnerable to known-plaintext attacks
    (see: http://math.ucr.edu/~mike/zipattacks.pdf)

- ***Standard*** and ***Strong*** – Uses Advances Encryption Standard (=AES, see: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard). 128-bit for *Standard*, 256-bit if *Strong* is selected.

  Description in attachment file dialog:
  - *Standard*: "Standard protection used by various programs like *WinZIP*. Considered secure given a long password"
  - *Strong*: "Strong encryption. Recipient needs MarvelZIP to unzip this archive"

Description for Strong is misleading and will be updated - most tools (aside form Windows Explorer that only supports password protected zip files) nowadays will handle the encryption method used by MarvelZip just fine.

Attachment Blocking



Attachment Blocking
File Restrictions
Conditions

Within these views you will find everything needed to set up your custom Attachment Blocking configuration. The view ***File Restrictions*** lists all such configurations for black- or whitelisting of when users add file attachments to IBM Notes documents.

For example, you can ensure that users do not attach files larger than a certain size, or that they may not attach any **.exe* and **.dll* files, or even create combined blocking rules, such as "no video files larger than 2 MB". Also, you can limit such restrictions to certain databases only, such as only mailfiles, all or files that belong to the CRM system, or similar. This allows you to flexibly create custom File Restrictions that match your different applications and respective requirements.

TIP

The action bar allows you to create new File Restrictions (Attachment Blocking Action). Within File Restrictions you are provided the option to **combine different file blocking Conditions**.

In the ***Conditions*** view, you find a list of all existing file blocking Conditions and corresponding **action bar** menu options to create your own Conditions: Filesize Definitions, Filename Patterns, Fingerprints (=tamper proof digital file patterns for filetype-detection; i.e. an **.exe* file, which was renamed to **.txt* will still be reliably detected as an **.exe* file) and Database Scope Conditions to limit File Restrictions to a certain (set of) database(s).

Filesize Definitions

Filesize Definitions are used to prevent too large (or too small) files from being attached to documents, such as emails or teamrooms for example.

Select one of the following scopes

- *If GREATER than…*
- *If smaller than…*

and specify the desired file size (in bytes).

Filename Patterns

Filename Patterns are used to prevent certain filenames from being attached to documents, such as emails, for example.

Select one of the following scopes

- *If filename MATCHes*
- *If filename does NOT match*

and specify one or multiple file patterns (using regular expression), such as **^(.*)\.exe$**.

Note that if you enter multiple patterns in one such Condition, only ONE of your entered filename patterns must match for the Condition to be met in an associated File Restriction.

Fingerprints

Fingerprints are used to prevent certain types of files from being attached to documents, such as emails – even if they are renamed (for example from *file.exe to file.txt*), fingerprints ensure proper detection of the respective file type.

Note that Fingerprints are also known as "Linux Magic Numbers" and there is a vivid community out there that regularly adds new fingerprints on various websites.

Select one of the following scopes

- *If fingerprint matches*
- *If fingerprint does NOT match*

Then specify the fingerprint pattern.