



**Monitor • Manage • Control • Secure**

## ContentKeeper Web Version 123.10 Release Notes

Overview 

---

These release notes are designed to provide a technical overview of new features and enhancements to ContentKeeper® Web Enterprise Version 123.10.

Copyright © 2000 - 2005 ContentKeeper Technologies

*ContentKeeper®*, *Closed Loop Collaborative Filtering™* and *TrickleFeed™* are trademarks of ContentKeeper Technologies. Copyright © 2000 - 2005, ContentKeeper Technologies, Canberra, Australia. All Rights Reserved.

Linux™ is a registered trademark of Linus Torvalds, Red Hat Linux® is a registered trademark of Red Hat Inc.

Cisco® is a registered trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

Intel® is a registered trademark of Intel Corporation and its subsidiaries in the United States and other countries.

eDirectory™, NDS and Novell® are trademarks of Novell Inc.

Microsoft®, Windows®, Windows NT and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Google™ and Google Image Search™ are trademarks of Google Inc.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products and specifications, configurations, and other technical information regarding the products contained in this manual are subject to change without notice. All statements, technical information, and recommendations contained in this manual are believed to be accurate and reliable but are presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this manual.

Document Designer and Author: Matthew R Richards

ContentKeeper Technologies  
218 Northbourne Avenue  
Braddon ACT 2612  
Australia  
PH +61-2-62614950  
Fax +61-2-62579801  
info@contentkeeper.com  
[www.contentkeeper.com](http://www.contentkeeper.com)

---

## ContentKeeper Release Notes

14<sup>th</sup> December 2005  
Document Revision C

These release notes apply to ContentKeeper® Web Enterprise Version 123.10 and include information on new features and enhancements between Version 123.00 and Version 123.10.

To find product changes specific to a particular version refer to the version index below.

### Table of Contents

<b>Version Index .....</b>	<b>4</b>
<b>Significant Changes .....</b>	<b>5</b>
<b>Filtering Control and Policies Blocking Rules .....</b>	<b>6</b>
Custom/Local Categories .....	6
Protocols .....	9
Authenticate State Settings .....	11
PSU Policy Summary .....	12
View Temporarily Bypassed URLs .....	13
Time of Day Saved Configurations .....	14
URL Reclassification Settings .....	14
Custom URLs.....	15
Custom URL Extensions.....	15
File Types.....	17
Other Rules .....	17
Custom Policies .....	19
<b>Domain Integration.....</b>	<b>20</b>
Workstation Authentication .....	20
eDirectory Username Resolution.....	21
LDAP/eDirectory User and Groups Setup.....	21
Staff Notification .....	22
Master/Slave Administration .....	24
<b>Logging and Reporting.....</b>	<b>25</b>
Syslog Configuration .....	25
<b>Setup and Customisation.....</b>	<b>26</b>
Web Interface Header .....	26
Time Zone .....	26
Excluded/Included IP Addresses .....	27
Miscellaneous Parameters.....	27

## Version Index

The version index lists all of the changes to ContentKeeper that are documented in these release notes in order of version with the most recent version first.

A page number accompanying a change indicates a section of this document that contains more detailed information about the change.

### ContentKeeper Version 123.10

- Custom/Local Categories – Page 6.
- Protocols – Page 9.
- Authenticate State Settings – Page 11.
- PSU Policy Summary – Page 12.
- View Temporarily Bypassed URLs – Page 13.
- Time of Day Saved Configurations – Page 14.
- URL Reclassification Settings – Page 14.
- Custom URLs – Page 15.
- Custom URL Extensions – Page 15.
- File Types – Page 17.
- Other Rules – Page 17.
- Custom Policies – Page 19.
- Workstation Authentication– Page 20.
- eDirectory Username Resolution – Page 21.
- LDAP/eDirectory User and Groups Setup – Page 21.
- Master/Slave Administration – Page 21.
- Staff Notification – Page 22.
- Syslog Configuration – Page 25.
- Web Interface Header – Page 26.
- Time Zone – Page 26.
- Excluded/Included IP Addresses – Page 27.
- Miscellaneous Parameters – Page 27.
- General enhancements have been made in the following areas of ContentKeeper:
  - NTP Synchronisation.
  - PSU Policy Blocking Rules.
  - Block/Unblock URLs in Control List.
  - Filtering of proxy encapsulated Internet traffic.
  - ContentKeeper Backups.
  - Management Port Proxy Settings.

## Significant Changes

This section of the release notes contains a list of the significant changes made in this release of ContentKeeper.

### Custom/Local Categories

The *Custom/Local Categories* facility introduces a new local URL Database of custom defined categories on the ContentKeeper Appliance.

Refer to page 6 for more information on the *Custom/Local Categories* facility.

### Protocols

The *Protocols* policy blocking rule has been completely re-designed and now includes a facility for creating custom protocol definitions.

Refer to page 9 for more information on the *Protocols* policy blocking rule.

### Custom Policies

The total number of possible custom policies has been increased from 100 to 200.

Refer to page 19 for more information on the custom policies.

### Workstation Authentication

*Workstation Authentication* is a new username resolution method that uses the HTTP Basic Authentication Scheme.

Refer to page 20 for more information on *Workstation Authentication*.

---

## Filtering Control and Policies Blocking Rules

This section of the release notes contains a technical overview of new features and enhancements to ContentKeeper that affect filtering control and Policies Blocking Rules.

### Custom/Local Categories

The new *Custom/Local Categories* facility significantly enhances the way ContentKeeper references URL classifications. Prior to the introduction of the *Custom/Local Categories* facility, a ContentKeeper Appliance would download a copy of the Global URL Database from the ContentKeeper Datacenter and store it locally.

The *Custom/Local Categories* facility introduces a new local URL Database on the ContentKeeper Appliance that is maintained separately from the Global URL Database. The new URL Database consists of 32 predefined Local categories that match the 32 categories in the Global URL Database, as well as the capacity to add up to 95 Custom categories.

*Custom/Local Categories* provides organisations with greater control over URL filtering and classification by allowing the creation of custom categories that contain URLs of a specific content type or related to a specific purpose.

#### Example 1.1 Custom Categories

If an organisation generally blocks the Advertising category but wishes to allow access to a specific set of sites it has contracted the services of; those sites can be added to a new custom category after which access may be granted to users on a per policy basis.

The *Custom/Local Categories* facility may be accessed by selecting *Custom/Local Categories* from the *Operational Settings* menu in the Web Interface.

Local categories and Custom categories are listed under separate tables in the *Custom Categories* menu. Within these tables is the index of each category, its description and the number of URLs that it contains.

Pre-Defined Local Categories					
Category Index	Category Description	URL Count	Category Index	Category Description	URL Count
1	Adult Content	0	17	www-Email Sites	0
2	News	0	18	Violence/Undesirable	0
3	Job Search	0	19	Malicious	0
4	Gambling	0	20	Search Sites	0
5	Travel/Tourism	0	21	Health Sites	0
6	Shopping	0	22	Clubs and Societies	0
7	Entertainment	0	23	Music Downloads	0
8	Chatrooms	0	24	Business Oriented	0
9	Dating Sites	0	25	Government Blocking List	0
10	Game Sites	0	26	Educational	0
11	Investment Sites	0	27	Advertising	0
12	E-Banking	0	28	Drugs/Alcohol	0
13	Crime/Terrorism	0	29	Computing/IT	0
14	Personal Beliefs/Cults	0	30	Swimsuit/Lingerie/Models	0
15	Politics	0	31	Spam	0
16	Sports	0	32	Reserved	0

Unlike the Local categories table which contains all 32 predefined Local categories, the Custom categories table contains only the categories that have been defined by the administrator. The Custom categories table grows with each new category that is defined.

Custom Defined Local Categories (101,102,103...196)			
Category Index	Category Description	URL Count	Delete Category
101	Project-1	5	<input type="checkbox"/>

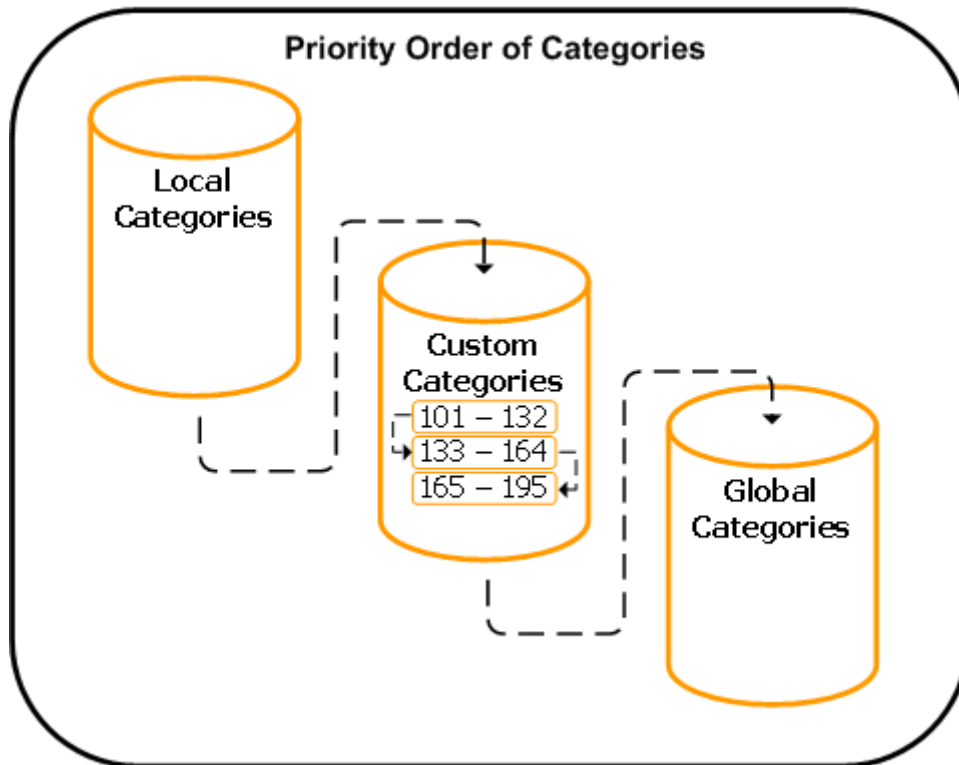
While the Global URL Database still functions as the primary Database of categorised URLs, any URLs added by the administrator are added directly to the Local or the Custom categories respectively before being submitted to the ContentKeeper Datacenter via the Closed Loop Collaborative Filtering™ system.

Also, any URLs reclassified by the administrator are moved from the Global Database to the Local or the Custom categories respectively before being submitted to the ContentKeeper Datacenter via the Closed Loop Collaborative Filtering™ system.

URLs categorised under the Local or the Custom categories take priority over those classified under the Global categories, and URLs categorised under Local categories take priority over those categorised under Custom categories.

Within the Custom categories, URL categories 101 to 132 take priority over categories 133 to 164, which in turn take priority over categories 165 to 196.

The following diagram illustrates the order of priority of the Local, Custom and Global categories.



The *Custom Categories* menu contains a facility for reporting on Local and Custom categories. This facility allows an administrator to view the contents of a category as well as monitor which users have added URLs to the category and how the URLs were added.

#	URL	Date Last Modified	By Username	Method
1	<a href="http://www.matchmaker.com">www.matchmaker.com</a>	20-Oct-2005,10:26 a.m.	admin	Reclassification
2	<a href="http://www.meetnewpeople.net">www.meetnewpeople.net</a>	20-Oct-2005,10:25 a.m.	admin	Manual Add/Modify
3	<a href="http://www.mydatingsite.com">www.mydatingsite.com</a>	20-Oct-2005,10:25 a.m.	admin	Manual Add/Modify

Additionally, the *Custom Categories* menu contains a facility for searching the Local URL Database. The facility allows administrators to specify a URL pattern to search for along with such parameters as modifying user, modification time frame and modification method.

**Search for a URL in  
Local/Custom URL Database**

Enter a Search string either as a full URL name, or partial URL name.  
(eg) **google** or **www.google.com** (Enter nothing to ignore)

**and**

Enter a User who made modifications (Select blank to ignore)

**and**

Select Modifications/Changes made during last (Select blank to ignore)

**and**

Select one of the following methods (Select blank to ignore)

Select Find URLs or Click Close Window to abort.

Please Wait...Searching for URLs matching the above search criteria...Done!

1 URLs matched the above Search Criteria!

#	Database	Index	Category	Description	URL	Date Last Modified	By Username	Method
1	Custom	101	Project-1		<a href="http://www.contentkeeper.com">www.contentkeeper.com</a>	20-Oct-2005,10:31 a.m	admin	Manual Add/Modify

## Protocols

The *Protocols* policy blocking rule allows administrators to report on and block the usage of a wide range of Internet protocols. In this version of ContentKeeper the *Protocols* policy blocking rule has been given a new interface. Support for a wider range of protocols has also been included along with a facility for defining custom protocols.

The enhanced *Protocols* policy blocking rule provides administrators with greater control over the use of Internet protocols within their organisation.

In the new *Protocols* policy blocking rule interface both predefined and user defined protocols are listed by type in individual tables. These tables include identification codes, protocol descriptions and help text for each protocol.

Instant Messaging					
#	Code	Protocol Description	Report	Block	Help
1	AIM	AOL Instant Messaging (AIM)	<input type="checkbox"/>	<input type="checkbox"/>	?
2	GOOGLETALK	Google Talk	<input type="checkbox"/>	<input type="checkbox"/>	?
3	JABBER	Jabber clients like Exodus	<input type="checkbox"/>	<input type="checkbox"/>	?
4	MSNCHAT	Microsofts MSN messenger	<input type="checkbox"/>	<input type="checkbox"/>	?

The list of predefined protocols has been increased to include the 8 protocol types listed below, with a total of 23 predefined protocol types:

- Instant Messaging
- Network OS
- Peer to Peer / File Sharing
- Proxy
- Web
- Mail and Cooperation
- Audio and Video Streams

and

- User Defined Protocols

Administrators may further enhance the list of protocols supported by ContentKeeper through the new User Defined Protocols facility. The facility allows administrators to specify TCP and UDP ports to define custom protocols.

User Defined Protocols	
Select Protocol Code Name	<input type="text"/>
Enter Protocol Code Name (Maximum 14 Characters)	<input type="text" value="P2PCOMMUNIT"/>
Protocol Description (Maximum 60 Characters)	<input type="text" value="Peer to peer file sharing"/>
TCP Port Numbers (Port numbers semi-colon separated)	<input type="text" value="3955"/>
UDP Port Numbers (Port numbers semi-colon separated)	<input type="text" value="3955"/>
Detail Description (1024 Characters)	
<input type="text" value="p2pCommunity is an Internet peer to peer file sharing protocol."/>	

The addition of time of day (TOD) settings to the *Protocols* policy blocking rule further increases the flexibility of filtering control offered by ContentKeeper. TOD settings let administrators allow or block protocol traffic between specific hours of the day.

Time of Day Settings							
Morning				Afternoon			
Midnight	to	1 A.M.	Allow	Noon	to	1 P.M.	Block
1 A.M.	to	2 A.M.	Allow	1 P.M.	to	2 P.M.	Block
2 A.M.	to	3 A.M.	Allow	2 P.M.	to	3 P.M.	Block
3 A.M.	to	4 A.M.	Allow	3 P.M.	to	4 P.M.	Block
4 A.M.	to	5 A.M.	Allow	4 P.M.	to	5 P.M.	Block
5 A.M.	to	6 A.M.	Allow	5 P.M.	to	6 P.M.	Block
6 A.M.	to	7 A.M.	Block	6 P.M.	to	7 P.M.	Block
7 A.M.	to	8 A.M.	Block	7 P.M.	to	8 P.M.	Allow
8 A.M.	to	9 A.M.	Block	8 P.M.	to	9 P.M.	Allow
9 A.M.	to	10 A.M.	Block	9 P.M.	to	10 P.M.	Allow
10 A.M.	to	11 A.M.	Block	10 P.M.	to	11 P.M.	Allow
11 A.M.	to	Noon	Block	11 P.M.	to	Midnight	Allow

## Authenticate State Settings

The *Authenticate State Settings* menu allows administrators to configure how users are authenticated when challenged by a ContentKeeper *Authenticate* blockpage. This menu replaces the *Site/Domain Authentication* menu under *Authentication* in the Web Interface,

The *Authenticate State Settings* menu introduces two new methods of authenticating users, increasing the flexibility of filtering control provided by ContentKeeper.

Authenticate Method	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #e0e0e0; padding: 2px;">Site-Domain Authentication (Via Cookies) ▾</div> <div style="background-color: #000080; color: white; padding: 2px;">Site-Domain Authentication (Via Cookies)</div> <div style="padding: 2px;">Source IP-Address Authentication</div> <div style="padding: 2px;">Resolved Username Authentication</div> </div>
---------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

These new methods allow administrators to change the way that *Authenticate* blockpages function, choosing between different methods of identifying authenticated users to suit the needs and network architecture of the organisation.

The new *Source IP Address Authentication* method identifies authenticated users on a per IP address basis. Once a request from a unique IP address is

authenticated, any further requests that are made from the IP address which would normally result in an *Authenticate* blockpage will not be blocked.

The new *Resolved Username Authentication* method identifies users on a per username basis. Once a user authenticates to an *Authenticate* blockpage, any further requests that are made by that user which would normally result in an *Authenticate* blockpage will not be blocked.

The *Site-Domain Authentication* method identifies authenticated users on a per site basis. Once a user authenticates to access a particular site, any further requests that are made by that user to that site which would normally result in an *Authenticate* blockpage will not be blocked.

## PSU Policy Summary

The *PSU Policy Summary* facility displays a summary of the Personal Surfing Unit (PSU) configuration settings for each of ContentKeepers filtering policies.

The *PSU Policy Summary* menu may now be accessed directly from the main menu of the ContentKeeper Web Interface instead of as a sub-menu to the *Create & Edit Policies* menu. This allows administrators to quickly review overall PSU settings and jump directly to individual users' PSU consumption and policy settings menus without having to navigate through other menus.

Current Status	Restart	Administration	Miscellaneous
Status Information	Restart ContentKeeper	Administration Accounts	Registration Details
Current Internet Activity	Reboot ContentKeeper Appliance	View Temporarily Bypassed URLs	Set/Adjust Date and Time
Current Blocking Activity	Shutdown ContentKeeper Appliance	Block/Unblock URLs in Control List	ContentKeeper Agent
Current Username Activity	ContentKeeper Anti-Spam	ContentKeeper Backups	Appliance Configuration Settings
View/Download Report Logs	ContentKeeper Anti-Virus	Audit Trail	Log Offloader
Dynamic Activity Viewer		Downloadable Modules	Category Aliases
Blocking/Reporting	General Settings	Operational Settings	Authentication
Create & Edit Policies	General Parameters	Management Port Proxy Settings	Authenticate State Settings
Display Policies	Excluded/Included IP Addresses	High Availability Module (H.A.M)	Departmental Report Setup
Verify Policy	Blockpage Customisation	URL Reclassification Settings	LOCAL Groups
Silent Mode Savings Report	Username Resolution	Bridge Device Settings	LDAP/eDirectory/AD Configuration
Webalizer Reports	Live Filtering Settings	Master/Slave Administration	PSU Policy Summary
Advanced Reporting Module	Syslog Configuration	Custom/Local Categories	



## View Temporarily Bypassed URLs

The *View Temporarily Bypassed URLs* menu allows you to view URLs for which filtering has been temporarily bypassed on your local ContentKeeper Appliance. This menu replaces the *View/Edit Reclassified URLs* menu under *Administration* in the Web Interface.

**View Temporarily Bypassed URLs**

This page is for URLs that have been Temporarily Bypassed (1 Hour to 12 Weeks).  
You can Temporarily Bypass URLs by clicking the **Submit URL** button on the ContentKeeper Block/Coaching page.  
Refer to [URL Reclassification Settings](#) to alter this behaviour.

Category Description is : **Temporarily Bypassed URLs**  
Category Index: **38**

URLs that may be viewed in this menu include those submitted by users for temporary reclassification. Refer to the *URL Reclassification Settings* menu under *Operational Settings* in the Web Interface for more information on how to enable temporary reclassification.

Temporarily Bypassed URLs						
#	URL	Category	User	Expiry Date	Status	Remove
1	<a href="http://www.hcf.com.au">www.hcf.com.au</a>	Health Sites	matt	15-Oct-2005,15:34	Expired	<input type="checkbox"/>
2	<a href="http://www.apex.org.au">www.apex.org.au</a>	Clubs and Societies	matt	25-Oct-2005,10:06	Allowed	<input type="checkbox"/>

The *View Temporarily Bypassed URLs* menu contains a list of all temporarily bypassed URLs, both current and expired, along with an option that allows each temporarily bypassed URL to be removed, i.e. revoked.

Reviewing the list of temporarily bypassed URLs allows administrators to determine if ContentKeepers *URL Reclassification Settings* have been properly configured and to immediately revoke any improperly bypassed URLs.

## Time of Day Saved Configurations

*Time of Day* settings are applied to ContentKeepers policy blocking rules under the *Create & Edit Policies* menu, and allow administrators to specify when a particular policy blocking rule is in effect.

The new *Time of Day Saved Configurations* facility at the bottom of the *Time of Day* settings screen gives administrators the ability to save and restore *Time of Day* settings to the *Categories*, *File Types* and *Custom URLs* menus.

This facility reduces the administrative overhead associated with ContentKeeper by allowing you to configure and save *Time of Day* settings in one policy and then restore them to any number of other policies.

Time of Day Saved Configurations	
Configuration Description	<input type="text"/>
Save Configuration and Redisplay	
Select/Apply Configuration	<input type="text"/>
Delete Selected Configuration	<input type="text"/>

## URL Reclassification Settings

ContentKeeper features a number of *URL Reclassification* facilities through which administrators and users are able to reclassify incorrectly classified URLs and classify new or non-managed URLs.

Details of each of the *URL Reclassification* facilities along with their configuration settings may be found in the *URL Reclassification Settings* menu.

The *URL Reclassification Settings* menu has been updated in this version of ContentKeeper to correspond with the new *View Temporarily Bypassed URLs* facility.

**Note:** Refer to the table of contents for more information on the new *View Temporarily Bypassed URLs* facility.

Enable URL Reclassification using all the above 4 Methods.	Yes <input type="checkbox"/> (Immediate on Local Server Only)
Password protect the above privileges. Click ' <b>Reclassification Users</b> ' button to add Users who have Reclassification Privileges.	Yes <input type="checkbox"/> (Local Server Only)
Provide Options to Temporarily Bypass URLs through Method (1)	1 Day <input type="text"/> (Local Server Only)
Reclassification Server	Local Server <input type="text"/>

## Custom URLs

The *Custom URLs* policy blocking rule allows administrators to configure filtering rules for specific URLs. Settings in the *Custom URLs* policy blocking rule override those in the *Categories* policy blocking rule, allowing administrators to configure filtering rules that target specific sites within a category.

*Custom URLs* has been enhanced to support port numbers. This means that an administrator may specify a port number as part of a URL pattern, allowing the creation of specific filtering rules that target web sites which are accessed over a non-standard HTTP port.

Index	URL	State	Settings
1	www.mysite.com:777/	Coach	Settings
2		Allow	Settings
3		Allow	Settings
4		Allow	Settings
5		Allow	Settings
6		Allow	Settings

## Custom URL Extensions

*Custom URL Extensions* enhance the functionality of the *Custom URLs* policy blocking rule by providing administrators with a convenient mechanism for creating and bulk importing URL clean lists into named URL groups, also known as *Custom URL Groups*.

The *Custom URL Extensions* facility is intended to be used primarily with *HTTP Request Methods* blocking facility to combat spyware and malware activity through the network gateway, refer to *Example 1.3 SSL Clean Lists* on page 18.

To access the new *Custom URL Extensions* facility, first view the *Global Policy* by browsing to the *Create & Edit Policies* menu and selecting *Global* from the *Select Policy* drop-down. Now browse to the *Custom URLs* policy blocking rule and click the *Custom URL Extensions* button. The *Custom URL Extensions* screen will pop up.

Cat #	Group Name	Group Description	# URLs	State	Edit	Import	Export	Report	Delete
51	eBanking	Authorised electronic banki	3	Ignore	Edit	Import	Export	Report	Delete
52			0	Ignore	Edit	Import	Export	Report	Delete

*Custom URL Groups* may either be created manually or bulk imported from CSV file.

*Custom URL Groups* are created manually by entering a name and a description into the *Custom URL Extensions* menu. URLs are then added to the new group manually with use of the *Edit* button, or imported with use of the *Import* button.

**Edit URLs**

Extension Name: **eBanking**

Description: **Authorised electronic banking sites**

URLs will be set to: **Ignore**

```

*.commbank.com.au*
*.national.com.au*
*.stgeorge.com.au*

```

Current number of URLs: **3**

*Custom URL Groups* are bulk imported from CSV file by clicking the *Bulk Import* button and following the prompts to upload the predefined *Custom URL Groups*.

**Note:** Instructions for creating a *Custom URL Groups* CSV file are included on the *Bulk Import* screen.

**Bulk Import URLs**

Warning! Bulk Importing URLs will replace all existing URLs.

**Upload Stage**

CSV file must be a comma delimited file with at least 2 columns.

**Column 1** must be the **Custom URL**, the URL format is described in the Main Custom URL Menu.

**Column 2** must be the **Custom URL Extension Name**, up to 16 Characters.

**Column 3** is the **Custom URL Extension Description** which is Optional, up to 64 characters.

**Column 4** is the **Custom URL State**, either **Ignore**, **Allow**, **Block**, **Coach**, or **Authenticate**.

Column 3 and 4 will default to Custom URL Extension Name and Custom URL State **Ignore** if either columns are undefined.

CSV filename must be of the form: (eg) filename.csv or filename.csv.gz, (etc).

**Browse** for your CSV URL Import file and then select **Upload** to have it first uploaded to your ContentKeeper Appliance.

## File Types

The *File Types* policy blocking rule allows administrators to configure filtering rules that target HTTP downloading of specific types of files. *File Types* has been enhanced and is now grouped into sections based upon the type of file and pre-configured with a greater number of file extensions.

A greater number of pre-configured file extensions can reduce the amount of time administrators spend configuring the *File Types* menu. Grouping the *File Types* menu into sections based upon the type of file the extensions belongs to simplifies the process of configuring filtering rules for any particular type of file content.

There are 15 different sections, each listed below, with a total of 102 pre-configured file extensions.

- Audio
- Video
- Interactivity
- Executable
- Programming Languages / Scripts
- Graphics
- Potentially Malicious
- Productivity
- Archives
- Installer
- Libraries
- Intermediate
- Cursor / Icon
- Test Files

and

- Other File Types

The *Other File Types* section contains provision for administrators to enter additional file extensions.

## Other Rules

The *Other Policy Rules* menu contains miscellaneous policy blocking rules that may be applied by an administrator when configuring ContentKeeper policies. This menu has been enhanced to include options for blocking *HTTP Request Methods*.

These new options increase ContentKeepers functionality by allowing administrators to manage HTTP GET, POST and CONNECT methods on non-standard ports.

HTTP Request Methods	
Block all HTTP GET Requests	Allow
Block all HTTP POST Requests	No
Block all HTTP CONNECT Requests (SSL)	Allow
	No
	Allow
	Block
	Coach
	Block Discard

The new options apply to all Internet traffic flowing through the ContentKeeper Bridge, not just the traffic on the ports specified under *Port Numbers for Filtering* in the *General Parameters* menu.

These options may be used in conjunction with the *Custom URLs* policy blocking rule to only allow users access to HTTP Web Servers that operate on port 80.

### Example 1.2 Only allow access to Web Servers over port 80

Restricting of Internet access to port 80 may be achieved for any policy by setting the *Block all HTTP GET Requests* and *Block all HTTP POST Requests* options to *Yes*, and then configuring a *Custom URL* of *\*:80* and setting it to *Allow*.

Another possible use of the new options, again in conjunction with the *Custom URLs* policy blocking rule, is to create an SSL clean list, only allowing users to make SSL connections to the specified web sites.

### Example 1.3 SSL Clean Lists

An SSL clean list may be created for any policy by setting the *Block all HTTP CONNECT Requests* option to *Yes* and then configuring the sites that you wish to allow users to access under *Custom URL Extensions*, e.g. *www.anz.com:443/\**

## Custom Policies

Custom policies allow administrators to tailor filtering rules to specific users or groups of users. The total number of possible custom policies has been increased from 100 to 200.

Support for an increased number of custom policies allows large organisations and organisations with a diverse or complex internal structure to better meet their filtering needs.

To create a new policy click on the "Clone" button (Maximum 200 Policies).

Policy Description	Default and Catch all Policy		
Select Policy	default	Clone	Report
Enable Policy	<input checked="" type="checkbox"/>	Delete	Verify
Policy Expiry	Never	15	Dec 2005

---

## Domain Integration

This section of the release notes contains a technical overview of new features and enhancements to ContentKeeper that affect network and domain integration facilities.

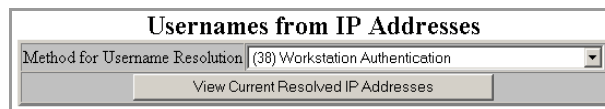
### Workstation Authentication

*Workstation Authentication* is a new username resolution method that uses the HTTP Basic Authentication Scheme to resolve usernames from individual workstation IP addresses.

*Workstation Authentication* is best suited to organisations that need to ensure accurate username resolution but do not have a suitable method, such as organisations without an authenticating proxy server or a directory service.

This new username resolution method is easily deployed as it requires no installation of additional software or reconfiguration of user workstations. *Workstation Authentication* can be configured to authenticate users against either a local database on the ContentKeeper Appliance or against an existing directory service.

To use *Workstation Authentication*, ContentKeeper username resolution must be configured to operate in *IP Address* mode. This can be achieved by selecting the *IP Address* radio button from the top of the *Username Resolution* menu. The *Workstation Authentication* option is then available as option (38) in the *Method for Username Resolution* drop-down, or as a secondary option to eDirectory under option (25).



The *Workstation Authentication* configuration settings may be accessed by clicking the *Workstation Authentication Settings* button in the *Advanced Username Resolution* menu; this will open the *Workstation Authentication Settings* menu in a new window.

---

**Note:** If the *Workstation Authentication Settings* button is greyed out, select *Workstation Authentication* from the *Method for Username Resolution* drop-down to make it accessible.

---

Use the *Workstation Authentication Settings* menu to configure settings for what users will be authenticated against and for how long, as well as to gain access to additional features such as *Idle Time*, which allows an administrator

to specify how long an IP address should be considered idle before ContentKeeper forces it re-authenticate.

Authenticate Against	Local Users
Authentication Period	4 Hours
Idle Time	5 Minutes
Login Pop-Up Message	ContentKeeper IP Authentication
Unauthenticated Username	Unauthenticated

The message displayed to users on the authentication pop-up may also be customised through the *Workstation Authentication Settings* menu, along with the username assigned to requests from users who have not yet authenticated.

## eDirectory Username Resolution

The eDirectory username resolution facility, which provides a mechanism for resolving usernames from Novell eDirectory, has been enhanced so that it will now query all specified eDirectory servers instead of just the first one it can bind to when attempting to resolve a username.

This enhancement improves the success rate of eDirectory username resolution in Novell environments where user authentication is distributed across multiple eDirectory servers.

## LDAP/eDirectory User and Groups Setup

*LDAP/eDirectory User and Groups Setup* provides administrators with a method of integrating ContentKeeper with many popular directory services, including Microsoft Active Directory, Novell eDirectory and OpenLDAP. The facility has been enhanced in this release of ContentKeeper through the addition of an *Advanced Active Directory Enumeration* option.

The new *Advanced Active Directory Enumeration* option improves support for Active Directory trees using nested groups by allowing ContentKeeper to recursively enumerate group membership.

*Advanced Active Directory Enumeration* may be enabled by browsing to the *LDAP/AD/eDirectory Enumeration* menu in the Web Interface, selecting *LDAP User/Group Enumeration* and then selecting the check-box at the bottom of the main table.

### LDAP/eDirectory Users and Groups Setup

<b>Server IP Address(es)</b> (Use semi-colon ';' as separator)	10.10.10.55
<b>Port Number(s)</b> (Use ' ' as separator)	3268 (Default is 389, For AD-GC:3268, For eD-SSL:636)
<b>Bind DN</b> (e.g cn=admin,o=Company)	cn=admin,cn=users,dc=contentkeeper,dc=com
<b>Bind Password</b>	***** Anonymous Bind <input type="checkbox"/> SSL Bind <input type="checkbox"/> (eDirectory Only)
<b>List of Search DN(s)</b> (e.g cn=staff,cn=users,dc=company,dc=com cn=students,cn=users,dc=company,dc=com) Please enter one Search DN per line. Maximum input length is 10,240 characters. Maximum length of each Search DN is 128 characters Maximum number of Search DN's is 250.	cn=staff,cn=users,dc=contentkeeper,dc=com cn=managers,cn=users,dc=contentkeeper,dc=com
Total Input Length: 74 Characters Number of Search DN's: 2	
<b>Filter</b> (e.g (objectCategory=person) or (objectClass=person))	(objectCategory=person)
<b>Enter one Group Type Attribute</b> (e.g memberOf or groupMembership)	memberOf
<b>Enter one User Type Attribute</b> (e.g cn or uid or sAMAccountName, etc)	sAMAccountName
<b>Group Name Format</b>	Group Name Only
<b>Automatic Enumeration</b>	Hourly (Takes effect once ContentKeeper <a href="#">Restarts</a> )

Remember to always click **Save and Redisplay** after making any menu changes!

Enable Advanced Active Directory Enumeration  
(Recursive Groups)

## Staff Notification

Local, federal or state legislation governing Internet access and censorship are becoming more and more common place. In some cases these laws require that staff/employees be notified that their Internet activity is being monitored and/or recorded. The new *Staff Notification* facility provides administrators with a method of delivering such a notification.

This facility allows administrators to choose how often users are notified and customise the look and feel of the notification.

The new *Staff Notification* facility is based on a customisable ContentKeeper *Coach* blockpage and as such may be accessed from the *Blockpage Customisation* menu in the Web Interface.

You can configure a Coach Page that can appear once a day warning Users they are being Filtered by ContentKeeper.

[Staff Notification](#)

Configuration is as simple as enabling the facility and choosing a display frequency of between one hour and one week from the drop-down menu. Customisation of the HTML coach page may also be done at this point.

### Staff Notification Coach Page

Staff Notification Options	
Enable	Yes ▾
Display Every	1 Day ▾

#### Staff Notification Coach Page

```

<html>
<head><title>ContentKeeper</title></head>
<body bgcolor='White' text='Black'>
<center><br><h1>ContentKeeper<br>Staff Notification</h1>
This is a reminder that you are being filtered by ContentKeeper!
<br><br>In accordance with our Internet Usage Policy, and complying with
<br>legislation, all Internet activity may be monitored.
<br>Inappropriate or non-business related sites may be blocked.
<br>Your Internet activity may be recorded and clicking on the link below
<br>acknowledges that you are aware of your responsibilities in accordance
<br><br><table border='1'>
<tr>

```

Size of Coach Page : **853** Bytes

**Note:** Four Variables can be substituted: {UriRaw}, {Url}, {Username}, and {Time}.

Select  to force the Staff Notification Coach Page to re-appear immediately for all Users. This also happens when ContentKeeper Restarts.

Select  to Display the Staff Notification Coach Page in a new window.

Once enabled, the new Staff Notification Coach Page may easily be tested by clicking the *Test Page* button at the bottom of the screen.

## ContentKeeper Staff Notification

This is a reminder that you are being filtered by ContentKeeper!

In accordance with our Internet Usage Policy, and complying with the appropriate legislation, all Internet activity may be monitored.

Inappropriate or non-business related sites may be blocked.

Your Internet activity may be recorded and clicking on the link below or refreshing this page acknowledges that you are aware of your responsibilities in accordance with our Internet Usage Policy.

URL	<a href="http://www.google.com.au/">http://www.google.com.au/</a>
Time	Thu Oct 13 18:31:00 2005
Username	matthew

## Master/Slave Administration

ContentKeepers *Master/Slave Administration* facility allows administrators to synchronise configuration settings on multiple ContentKeeper Appliances. The facility has now been enhanced by including the option to synchronise the *Custom/Local URL Database*, adding support for the new *Custom/Local Categories* facility.

---

**Note:** Refer to the table of contents for more information on the new *Custom/Local Categories* facility.

---

The option to synchronise the *Custom/Local URL Database* simplifies management of multiple ContentKeeper Appliances and reduces administrative overhead.

The new option is located under *Synchronisation Options* in the *Master/Slave Administration* menu on ContentKeeper Appliances configured as a master.

**Master/Slave Administration**

**Manual Synchronization Options**

(These options are synchronized when the **Sync** button is clicked.  
The Slave Appliance will Restart once for each synchronization action.)

<input type="checkbox"/> All Policies	<input type="checkbox"/> Local Groups
<input checked="" type="checkbox"/> Custom/Local URL Database	<input type="checkbox"/> Block Page Customization
<input type="checkbox"/> Exclude/Include IP Addresses	<input type="checkbox"/> Date/Time Synchronization
<input type="checkbox"/> Windows Agent	<input type="checkbox"/> LDAP/eDirectory Groups

Additionally, when ever the *Master/Slave Administration* facility is enabled, a message will appear at the top of the Web Interface main menu warning of the fact that SSH has been enabled on the ContentKeeper Appliance.

**Note: SSH is Currently Enabled.**

---

## Logging and Reporting

This section of the release notes contains a technical overview of new features and enhancements to ContentKeeper that affect its logging and reporting facilities.

### Syslog Configuration

The *Syslog Configuration* facility allows *Internet Activity Logs* and *Audit Logs* to be streamed to a remote syslog host in real-time. A new option included with the *Syslog Configuration* facility allows the MAC address of each source IP address to be included with the syslog output.

Mac addresses are appended to IP address in the Internet Activity Logs providing administrators with more accurate identification of the source of web requests.

Do you want to append the MAC Address to the IP Address? (i.e IP/Mac)

## Setup and Customisation

This section of the release notes contains a technical overview of new features and enhancements to ContentKeeper that affect its setup and customisation facilities.

### Web Interface Header

The ContentKeeper Web Interface header provides a quick reference to information about a ContentKeeper Appliance including such items as the software version and the management port IP address.

The addition of the *License Type*, *License Left* and *Users Licensed* fields to the Web Interface header allows administrators to quickly and easily determine their license type and how much time remains before it expires as well as how many users their ContentKeeper Appliance is licensed for.

```
Version: 123.10 Build Date: 06-Dec-2005 Hostname: ContentKeeper IP-Address: 192.9.200.81  
Company: ContentKeeper Technologies Registration ID: 61-02-14259 Username: admin  
License Type: Full License License Left: 365 Day(s) Users Licensed: 5000
```

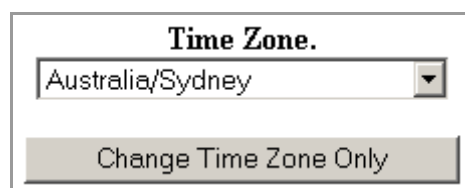
The Web Interface header may be found at the top of most ContentKeeper Web Interface menus.

### Time Zone

The new *Time Zone* facility allows administrators to configure the time zone of a ContentKeeper Appliance from within the Web Interface.

This facility simplifies the task of configuring a time zone by replacing command line tools with an easy to use drop-down menu.

The *Time Zone* facility is accessible through the *Set/Adjust Date and Time* menu. To set the time zone, simply select an option from the drop-down menu and then click the *Change Time Zone Only* button.



The screenshot shows a web interface for configuring the time zone. At the top, the text "Time Zone." is displayed. Below it is a drop-down menu with "Australia/Sydney" selected. At the bottom of the interface is a button labeled "Change Time Zone Only".

## Excluded/Included IP Addresses

The *Excluded/Included IP Addresses* facility allows an individual IP address or ranges of addresses to be explicitly excluded from or included in filtering. A *Comment/Description* field has been added to this facility.

The new *Comment/Description* field allows administrators to quickly identify an individual IP address or ranges of addresses without having to refer to lists or tables or physically locate the system to which they belong.

IP Address	IP Range Mask	Mode	Comment/Description
192.168.0.104	255.255.255.255	Excluded ▾	Anti Virus Update Server
10.10.10.0	255.255.255.128	Excluded ▾	Development Network
	255.255.255.255	▾	
	255.255.255.255	▾	
	255.255.255.255	▾	

The *Excluded/Included IP Addresses* menu is accessible under *General Settings* in the ContentKeeper Web Interface main menu.

## Miscellaneous Parameters

ContentKeepers *Miscellaneous Parameters* allow administrators to configure the settings for various ContentKeeper blocking functions, such as how it filters image components and which HTTP error code is given with a blockpage.

Two new options have been added to Miscellaneous Parameters. The first option allows administrators to configure the Coach blockpage frequency; this allows the behaviour of Coach blockpages to be tailored to the needs of individual organisations. The second option allows administrators to configure Blockpage Customisation settings separately for Coaching of SSL sites, avoiding complications that may arise from sites with strict access restrictions.

*Miscellaneous Parameters* may be access by browsing to the *General Parameters* menu and clicking on the *Miscellaneous Parameters* button.

The *Coach Blockpage Frequency for all Sites* option allows an administrator to choose a browse window setting of between 5 and 300 seconds.

<b>Miscellaneous Parameters</b>	
Replace Google Thumb Images	Yes
Replace Image Components	Yes
HTTP Header Error Code for Block Pages	403 Forbidden
Block JavaScript URLs with HTML or JavaScript	JavaScript
Coach Block Page Frequency for all Sites	60 Seconds
Coach Block Page for SSL Sites	5 Seconds 15 Seconds 30 Seconds <b>60 Seconds</b> 120 Seconds 180 Seconds 240 Seconds 300 Seconds

Some SSL sites (e.g. Internet Banking Sites) have access restrictions based on the referrer site, using a *Redirect Custom Blockpage* may make it impossible to access these SSL sites. The *Coach Block Page for SSL Sites* option allows an administrator alter the blockpage customisation method specifically for SSL sites to combat this.

<b>Miscellaneous Parameters</b>	
Replace Google Thumb Images	Yes
Replace Image Components	Yes
HTTP Header Error Code for Block Pages	403 Forbidden
Block JavaScript URLs with HTML or JavaScript	JavaScript
Coach Block Page Frequency for all Sites	60 Seconds
Coach Block Page for SSL Sites	Redirect Simple Default <b>Redirect</b>