Content Filtering Service Configuration

This chapter describes how to configure content filtering support with ECS.

In this chapter, only the minimum set of configurations required to make the system operational with content filtering services are provided. Additional configuration commands specific to the content filtering service are available in the *Command Line Interface Reference*.

The following topics are described in this chapter:

Configuring the System for Content Filtering Support

This section lists the high-level steps to configure a system with Content Filtering service in conjunction with the Enhanced Charging Services.

Caution Before proceeding with the configuration, refer the *Additional Requirements on Chassis for Content Filtering* section of the *Content Filtering Support Overview* chapter for the minimum system requirements. If the system has fewer than two processing cards, Content Filtering service cannot be activated on the system.

Step 1 Set the initial configuration parameters such as activating the processing cards and creating the VPN context by applying the example configurations in Initial Configuration, on page 2.

Step 2 Enable the Enhanced Charging Service with Content Filtering, and configure Content Filtering parameters:

- For URL Blacklisting support, enable the Enhanced Charging Service by applying the example configurations presented in URL Blacklisting Configuration, on page 3.

–and/or–

- For Category-based Content Filtering support, enable the Enhanced Charging Service by applying the example configurations presented in Category-based Content Filtering Configuration, on page 5.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Initial Configuration

Step 1 Configure the processing cards in the chassis by applying the example configuration in Activating Processing Cards, on page 2.

Step 2 Configure system management parameters in the local context by applying the example configuration in Modifying the Local Context, on page 2.

Step 3 Create the VPN context and interface by applying the example configuration in Creating the VPN Context, on page 3.

Step 4 Create the service within the newly created context by applying the example configuration in the *Service Configuration* chapter of the *System Administration Guide*.

Activating Processing Cards

The following example activates two processing cards, placing one in active mode and labeling the other as redundant:

```
configure
   card slot_number
      redundancy card-mode
      exit
   card slot_number
      mode active pac
      end
```

Modifying the Local Context

The following example sets the default subscriber in the local context:

```
configure
   context local
      interface local_ctx_iface_name
         ip address ip_address ip_mask
         exit
      server ftpd
         exit
      server telnetd
         exit
      subscriber default
         exit
      administrator name encrypted password password ftp
      ip route ip_addr ip_mask next_hop_addr local_ctx_iface_name
      exit
   port ethernet slot#/port#
      no shutdown
```

```
    bind interface local_ctx_iface_name local
    exit
end
```

Creating the VPN Context

The following example creates the VPN context and interface and binds the VPN interface to a configured Ethernet port:

```
configure
  context vpn_context_name -noconfirm
    interface vpn_interface_name
      ip address ip_address ip_mask
      exit
   subscriber default
      exit
    ip route 0.0.0.0 0.0.0.0 next_hop_address vpn_interface_name
    exit
  port ethernet slot_number/port_number
    no shutdown
    bind interface vpn_interface_name vpn_context_name
    end
```

URL Blacklisting Configuration

This section describes steps to configure the system for URL Blacklisting support.

Step 1 Enable the ACS subsystem by applying the example configuration in Enabling ACS Subsystem, on page 3.

Step 2 Configure URL Blacklisting database parameters by applying the example configuration in Configuring URL Blacklisting Database Parameters, on page 4.

Step 3 Create the Active Charging Service, and set URL Blacklisting matching method by applying the example configuration in Creating Active Charging Service and Setting URL Blacklisting Matching, on page 4.

Step 4 Enable URL Blacklisting functionality in a rulebase, and configure the action to be taken by applying the example configuration in Enabling URL Blacklisting in Rulebase and Configuring Blacklisting Action, on page 4.

Step 5 Load/upgrade URL Blacklisting database by applying the example configuration in Loading/Upgrading URL Blacklisting Database, on page 4.

Enabling ACS Subsystem

Use the following configuration to enable the Active Charging Service subsystem for URL Blacklisting:

```
configure
  require active-charging
  end
```

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Configuring URL Blacklisting Database Parameters

Use the following configuration to configure URL Blacklisting database parameters:

```
configure
   url-blacklisting database directory path directory_path
   url-blacklisting database max-versions max_versions
   url-blacklisting database override file file.extension
   end
```

Creating Active Charging Service and Setting URL Blacklisting Matching

Use the following configuration to create the Active Charging Service and set URL Blacklisting match:

```
configure
  active-charging service service_name [ -noconfirm ]
     url-blacklisting match-method { exact | generic }
     end
```

Enabling URL Blacklisting in Rulebase and Configuring Blacklisting Action

Use the following configuration to enable URL Blacklisting in a rulebase and configure the blacklisting action:

```
configure
   active-charging service service_name
      rulebase rulebase_name [ -noconfirm ]
        url-blacklisting action { discard | redirect-url url | terminate-flow
 | www-reply-code-and-terminate-flow reply_code }
         end
```

Loading/Upgrading URL Blacklisting Database

Use the following command to load/upgrade the URL Blacklisting database:

```
upgrade url-blacklisting database [ -noconfirm ]
```

Testing URL Blacklisting Functionality

The URL Blacklisting functionality can be tested by appending test URLs/URIs to the blacklist file. The test URLs/URIs must be added to the *testurldb.pub* file in the *<WEM_Install_Dir>/flash/blacklist/testurldb* directory.

The *testurldb.pub* file must have one URL per line without space. If space is included in the URL entries, the WEM ignores the URLs with space.

Category-based Content Filtering Configuration

This section describes the steps to configure the system for Category-based Content Filtering support.

Step 1 Enable the Enhanced Charging mode for Category-based Static Filtering by applying the example configuration in Enabling ACS Subsystem, on page 5.

Step 2 Configure the global parameters like database path and version for Content Filtering service by applying the example configuration in Configuring Content Rating Rule Database Parameters, on page 5. This is an optional step. In case this configuration is not performed, the default values will be used.

Step 3 Create the Active Charging Service and Content Filtering Policy by applying the example configuration in Creating Active Charging Service and Content Filtering Policy, on page 6.

Step 4 Configure the Content Filtering Policy Identifier and actions by applying the example configuration in Configuring Content Filtering Policy, on page 6.

Step 5 *Optional*. Create billing and charging actions by applying the example configuration in the *Configuring Enhanced Charging Services* chapter of the *Enhanced Charging Services Administration Guide*.

Step 6 *Optional*. Define rule definitions by applying the example configuration in the *Configuring Enhanced Charging Services* chapter of the *Enhanced Charging Services Administration Guide*.

Step 7 Create and configure the rulebases by applying the example configuration in Configuring Rulebase for Content Filtering, on page 6. For more information on rulebase configuration, refer to the *ECS Configuration* chapter in the *Enhanced Charging Services Administration Guide*.

Step 8 Apply the Content Filtering service to subscribers/APNs by applying the example configuration in #unique_51/#unique_52.

Step 9 Create the EDR format and configure attributes by applying the example configurations in Configuring Event Detail Record (EDR), on page 7.

Enabling ACS Subsystem

Use the following configuration to enable the Active Charging Service subsystem:

```
configure
  require active-charging content-filtering category
  end
```

Notes:

A reboot is essential when enabling/disabling Category-based Content Filtering using the **require active-charging content-filtering category** command.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Configuring Content Rating Rule Database Parameters

Use the following configuration to configure Content Rating Rule database parameters:

```
configure
   content-filtering category database directory path directory_path
   content-filtering category database max-versions max_versions
   content-filtering category database override file file.extension
   end
upgrade content-filtering category { database | rater-pkg }
```

Creating Active Charging Service and Content Filtering Policy

Use the following configuration to create the Active Charging Service and Content Filtering Policy:

```
configure
   active-charging service service_name [ -noconfirm ]
     content-filtering category policy-id cf_policy_id [ description description
 ] [ -noconfirm ]
      end
```

Configuring Content Filtering Policy

Use the following configuration to configure the content filtering policy:

```
configure
   active-charging service service_name
      content-filtering category policy-id cf_policy_id
       analyze priority priority { all | category category | x-category x-category
 } action { allow | content-insert content_string | discard | redirect-url url
| terminate-flow | www-reply-code-and-terminate-flow reply_code } [ edr
edr_format ]
        failure-action { allow | content-insert content_string | discard |
redirect-url url | terminate-flow | www-reply-code-and-terminate-flow
reply_code } [ edr edr_format ]
        end
```

Notes

- To configure runtime categories not present in the CLI, use the following command:

  analyze priority *priority* **x-category** *x-category* **action** { **allow** | **content-insert** *content_string* | **discard** | **redirect-url** *url* | **terminate-flow** | **www-reply-code-and-terminate-flow** *reply_code* } [**edr** *edr_format*]

- To configure the action to take for any match, and the default action to take when the category returned after rating is not configured in the subscriber's content filtering policy, use the following command:

  analyze priority *priority* **all action** { **allow** | **content-insert** *content_string* | **discard** | **redirect-url** *url* | **terminate-flow** | **www-reply-code-and-terminate-flow** *reply_code* } [**edr** *edr_format*]

Configuring Rulebase for Content Filtering

Use the following configuration to configure the rulebase:

```
configure
   active-charging service service_name
     rulebase rulebase_name
       route priority route_priority ruledef ruledef_name analyzer analyzer_name
```

```
[ description description ]
        action priority priority { { group-of-ruledefs group_name | ruledef
ruledef_name } charging-action charging_action_name [ description description ] }
        flow end-condition content-filtering edr edr_format_name
        billing-records { egcdr | radius | udr udr-format format_name } +
        content-filtering category policy-id cf_policy_id
        content-filtering mode category { static-only }
        end
```

Enabling Category-based Content Filtering Support

APN Configuration

Use the following configuration to apply Content Filtering configuration to an APN through policy identifier:

```
configure
  context context_name
    apn apn_name
      content-filtering category policy-id cf_policy_id
      end
```

Subscriber Configuration

Use the following configuration to apply Content Filtering configuration to a subscriber through policy identifier:

```
configure
  context context_name
    subscriber name user_name
      content-filtering category policy-id cf_policy_id
      end
```

Important When changing the *cf_policy_id* included in RADIUS CoA and CCA/RAR messages from AAA/PCRF, it is observed that the CF policy ID is applied to subscriber session level even if it is set at rulebase level or APN level. That is, the policy ID set by the latest message takes precedence and the same value is applied at the session level.

Important Category Policy ID applied to APN or subscriber in this mode overrides the Category Policy ID configured using the **content-filtering category policy-id** *cf_policy_id* command in the *Configuring Rulebase for Content Filtering* section.

Configuring Event Detail Record (EDR)

This section describes how to configure Category-based Content Filtering EDR settings. The system does not generate URL Blacklisting specific EDRs.

To configure Category-based Content Filtering EDR settings:

Step 1 Enable the EDR module and file format for EDR in context configuration mode by applying the example configuration in EDR Module Configuration, on page 8.

Step 2 Define attributes and rule variables by applying the example configuration in EDR Attribute Configuration, on page 8.

Step 3 *Optional*. Enable charging record retrieval by applying the example configuration in the *Enabling Charging Record Retrieval* section of *Enhanced Charging Services Administration Guide*.

EDR Module Configuration

Use the following configuration to enable EDR module and configure the file for EDR generation in Content Filtering services:

```
configure
  context context_name
    edr-module active-charging-service
      file [ edr-format-name ] [ name file_name ]+
      end
```

Notes:

For more information on keywords/options available with the **file** command, refer to the *EDR Module Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

EDR Attribute Configuration

Use the following configuration to configure attributes and rule-variables for EDRs for Content Filtering services:

```
configure
  active-charging service service_name
    edr-format edr_format_name
      attribute attribute priority priority
      rule-variable protocol rule priority priority
      end
```

Notes:

For more information on options available with **attribute** and **rule-variable** commands, refer to the *EDR Format Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Verifying the Configuration

This section describes how to review the configurations after saving them in a .cfg file, and to retrieve errors and warnings within an active configuration for a service.

Viewing System Configuration

Use the following configuration to view the active configuration for a service:

```
configure
  context context_name
```

```
   end
show configuration
```

Viewing Service Configuration Errors

Use the following configuration to view the errors in configuration for a service:

```
configure
   context context_name
   end
show configuration errors verbose
```

This command also shows the ambiguities in configurations with Content Filtering service, category, and rulebase configuration. Warnings/errors are displayed in the following scenarios:

- Warning: When **require active-charging content-filtering category** CLI command is not activated and any Content Filtering configurations are done.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

- Error: When Content Filtering is enabled, but no Content Filtering Policy ID is configured in the Active Charging Service.
- Error: A rulebase uses an undefined Content Filtering Policy ID.
- Error: A rulebase has Content Filtering Category Mode set, but Content Filtering Policy ID is not set.
- Warning: A rulebase has Content Filtering Policy ID set, but Content Filtering Category Mode is not set.
- Error: An APN uses a Content Filtering Policy ID not defined in the Active Charging Service.
- Error: A subscriber uses a Content Filtering Policy ID not defined in the Active Charging Service.
- Warning: When no default analyze rule is configured in Content Filtering Policy ID.
- Warning: When default analyze rule is configured in the Content Filtering Policy ID, but not at the lowest priority.
- Warning: When no analyze rule is configured in Content Filtering Policy ID.

Gathering Statistics

This section explains how to gather statistics and configuration information for:

URL Blacklisting Statistics

This section explains how to gather URL Blacklisting statistics and configuration information.

In the following table, the first column lists what statistics to gather, the second column lists the action to perform, and the third column describes what information is displayed or what information to look for in the resulting output.

Table 1: Gathering URL Blacklisting Statistics and Configuration Information

Statistics Wanted	Action to Perform
To view URL Blacklisting statistics, optionally for rulebase(s)	**show active-charging url-blacklisting statistics** [**rulebase** {**all** | **name** *rulebase_name* }] [**verbose**] [| { **grep** *grep_options* | **more** }]
To view URL Blacklisting static database configuration	**show url-blacklisting database** [**all** | **url** *url* | **facility acsmgr** { **all** | **instance** *instance* }] [**verbose**] [| { **grep** *grep_options* | **more** }]
To view total Blacklisting URL hits and misses statistics, optionally for rulebase(s) or specific ACS instance	**show active-charging subsystem** { **all** | **facility acsmgr** [**all** | **instance** *instance*] | **full** } | **rulebase name** *rulebase_name*] | [| { **grep** *grep_options* | **more** }]
To view information for rulebase(s) configured in a system or service	**show active-charging rulebase** { **all** [**service name** *svc-name*] | **name** *rulebase-name* [**service name** *svc-name*] | **statistics** [**name** *rulebase-name*] } | [| { **grep** *grep_options* | **more** }]
To view ACS session statistics	**show active-charging sessions all** [| { **grep** *grep_options* | **more** }]

Category-based Content Filtering Statistics

This section explains how to gather Category-based Content Filtering statistics and configuration information.

In the following table, the first column lists what statistics to gather, the second column lists the action to perform, and the third column describes what information is displayed or what information to look for in the resulting output.

Important For more information on Content Filtering statistics collection, refer to the *Exec Mode Commands* chapter of the *Command Line Interface Reference*.

Table 2: Gathering Category-based Content Filtering Statistics and Configuration Information

Statistics Wanted	Action to Perform
To view Category-based Content Filtering database statistics/configuration	**show content-filtering category database** [**active** | **all** | **facility srdbmgr** { **all** | **instance** *instance* } | **url** *url_string*] [**verbose**] [| { **grep** *grep_options* | **more** }]
To view Category-based Content Filtering category statistics	**show content-filtering category statistics** [**facility srdbmgr** { **all** | **instance** *instance* }] [| { **grep** *grep_options* | **more** }]

Statistics Wanted	Action to Perform
To view information of a database URL for Category-based Content Filtering application in a service	**show content-filtering category url** *url_string* [**policy_id** *cf_policy_id* | **rulebase** *rulebase_name*] [**verbose**] [| { **grep** *grep_options* | **more** }]
To view Content Filtering Server Group (CFSG) details configured in the service	**show content-filtering server group** [**statistics**] [**name** *cfsg_name*] [| { **grep** *grep_options* | **more** }]
To view Category-based Content Filtering category policy definitions	**show active-charging content-filtering category policy-id** { **all** | **id** *policy_id* } [| { **grep** *grep_options* | **more** }]
To view Category-based Content Filtering statistics, optionally for rulebase(s)	**show active-charging content-filtering category statistics** [**rulebase** { **name** *rulebase_name* | **all** }] [**verbose**] [| { **grep** *grep_options* | **more** }]
To view details of Content Filtering Server Group (CFSG) configured in the service	**show active-charging content-filtering server-group** [**statistics** [**verbose**]] [**name** *cfsg_name*] [| { **grep** *grep_options* | **more** }]
To view information for rulebase(s) configured in a system or service	**show active-charging rulebase** [**all** [**service name** *svc_name*] | **name** *rulebase_name* [**name** *cfsg_name*] [| { **grep** *grep_options* | **more** }]
To view Active Charging session statistics	**show active-charging sessions all** [| { **grep** *grep_options* | **more**}]

Supported Bulk Statistics

For information on bulk statistics configuration and collection, and the list of bulk statistics for the Content Filtering service, refer to the *Bulk Statistics Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Supported Thresholds and SNMP Traps

The CF traps related to embedded/StarOS CF are available in the chassis MIB file. The CF Applications specific traps related to WEM processes like DB conversion, merging, etc. are now packaged with the WEM MIB file.

For information on the SNMP traps and thresholds for the Content Filtering service, see the *Content Filtering Application MIB* chapter of the *SNMP MIB Reference*.

For information on configuring CF thresholds, see the *Content Filtering Thresholds* chapter of the *Thresholding Configuration Guide*.