



QUICK START GUIDE



Cisco Service Control URL Blacklisting Solution Guide, Release 3.7.x

- 1** Managing URL Blacklists Using the Cisco Service Control Engine Platform
- 2** Configuring User Authorization
- 3** Managing the sce-url-database
- 4** Enabling Deep HTTP Inspection
- 5** URL Normalization
- 6** Protected URL Database Configuration Example
- 7** Obtaining Documentation and Submitting a Service Request



Note This document supports all 3.7.x releases.

1 Managing URL Blacklists Using the Cisco Service Control Engine Platform

The Cisco Service Control Engine (SCE) platform-managed URL database resides on the Cisco SCE platform. The URL database, `sce-url-database`, is managed by using CLI commands rather than the Cisco Service Control Application for Broadband (Cisco SCA BB) Console. In addition to the advantage of having a separate URL database that is configurable directly by CLI commands, this database can be used to hide a list of URLs to prevent them from being accessed by the Console or the CLI.

The URL database must be declared as a separate flavor in the Cisco SCA BB application, but all the other configuration and management tasks are performed using the CLI.

The URL database can be protected. As part of protecting the `sce-url-database`, one user is designated as the owner of the database and only that user can execute the CLI commands on the database. Protection involves defining the authentication, authorization, and accounting (AAA) method (either based on local users or on a TACACS+ server, and so forth) and defining at least one user to be the owner of the database. For further details about the configuration, see the “Configuring the Management Interface and Security” chapter of the [Cisco SCE 8000 10GBE Software Configuration Guide](#) or the “Configuring the Management Interface and Security” chapter of the [Cisco SCE 8000 GBE Software Configuration Guide](#).

After the database is configured to be protected, no database information, (including information about the owner, database entries, authorization information, and the relevant saved configuration in the log files and in the relevant Cisco SCA BB reports, is accessible to any user. The database owner can change the authorizations by using the CLI. However, when any of the protection rules are relaxed (or all of the protection rules are relaxed by removing them) the database is reset automatically.

To protect the secrecy of the database information, the database entries can be imported to Cisco SCE (by using the CLI) in an encrypted form with the 128-bit key length Advanced Encryption Standard (AES). The key can be set or updated by using the appropriate CLI command; typically, this command should be run over a secure Telnet session.

There are two general categories of CLI commands related to the Cisco SCE-managed URL database:

- User authorization commands
- Database management commands

2 Configuring User Authorization

The sce-url-database can be managed by a single authorized user, who is the designated owner of this database.

- If there is no designated owner, the sce-url-database is unprotected and the contents can be read and modified by any user.
- If there is a designated owner, the sce-url-database is protected. The default protection settings are as follows:
 - Read permission—no-user. This setting is not configurable.
 - Write permission—owner-only. The owner can configure this setting to all the users.
 - Lookup permission—no-user. The owner can configure this setting only to the owner.
 - Encryption key—no-key. The owner can configure an encryption key.

User Authorization Guidelines

These are some of the guidelines for user authorization:

- The default user cannot be the owner.
- Only the owner can configure the protection settings. If there is no owner, the database is unprotected, and all the users have read and write permission. A user can be made the designated owner of the database only if the database does not have a designated owner.
- When a protection setting is relaxed, the database is reset automatically. Protection can be relaxed as follows:
 - Protection can be removed completely by using the **no sce-url-database protection** command.
 - Write permission can be changed from owner-only to all-users.
 - Lookup permission can be changed from no-user to owner-only.
- The sce-url-database configuration information cannot be accessed from the running config and startup config file:
 - Protected information is not displayed when a **show** or **more** command is executed on the config files.
 - Protected information is displayed when a **copy** command is executed on the config files.

How to Specify a New Owner for the sce-url-database

To specify a new owner for the sce-url-database, use the following command in the interface linecard configuration mode (config if):

```
sce-url-database protection owner (myself | (name user-name))
```

The authorization level required by a user to perform this task is Admin.

Prerequisites

If an owner is already assigned to the sce-url-database, that owner must first remove the owner designation using the **no sce-url-database protection** command, which removes all database protection (see the [“How to Remove All the Protection Rules for the sce-url-database”](#) section on page 5).

Options

The following options are available to specify a new owner in the sce-url-database:

- **myself**—The owner of the database who is currently logged in. The user should not log in using the default username.
- **user-name**—The user that is to be designated as the owner of the database. The default username cannot be used. When specifying a *user-name*, if no such user exists (either in the local database or if in the TACACS+ server) or if the AAA authorization is not configured accordingly (that is, the logic user), there is no effective way of utilizing the permissions granted to this owner. Only after the relevant user or AAA settings are configured do the permissions of the owner user become effective.

Default

No owner is specified.

Results

The following are the results available after specifying a new owner in the sce-url-database:

- The specified user *user-name* is the owner of the sce-url-database.
- Read permission to the sce-url-database is not permitted for any user (including the owner).
- No Raw Data Records (RDRs) or traps contain data pertaining to the URLs in the sce-url-database.
- By default, only the owner has write permission to the sce-url-database.
- By default, none of the users, including the owner, can perform the lookup action..

How to Configure Write Protection for the sce-url-database

To configure write protection for the sce-url-database, use the following command in the interface linecard configuration mode (config if):

sce-url-database protection allow-write (all-users | owner-only)

This command can be executed only by the assigned owner of the sce-url-database. The authorization level required by a user to perform this task is Admin.

Prerequisites

A person should already be assigned as the owner of the sce-url-database.

Options

The following options are available to configure write protection in the sce-url-database:

- all-users
- owner-only

Default

The following are the default settings available while configuring write protection in the sce-url-database:

- If no owner is assigned, the default is **all-users**.
- If an owner is been assigned, the default is **owner-only**.

Results

If protections are relaxed (changed from owner-only to all-users), the sce-url-database is reset automatically.

How to Configure Lookup Protection for the sce-url-database

To configure lookup-protection for the sce-url database, use the following command in the interface linecard configuration mode (config if):

sce-url-database protection allow-lookup (owner-only | no-user).

This command can be executed only by the assigned ownerof the sce-url-database. The authorization level required by a user to perform this task is Admin.

Prerequisites

An owner should already be assigned to the sce-url-database.

Options

The following options are available to configure lookup protection in the sce-url-database:

- owner-only
- no-user

Default

The following are the default settings available while configuring lookup protection in the sce-url-database:

- If no owner is assigned, the default is **all-users**.
- If an owner is assigned, the default is **no-user**.

Results

If protections are relaxed (changed from no-user to owner-only), the sce-url-database is reset automatically.

How to Configure the sce-url-database Encryption Key

To configure the sce-url-database encryption key, use the following command in the interface linecard configuration mode (config if):

sce-url-database protection encryption-key *encryption-key*

This command can be executed only by the assigned owner of the sce-url-database. The authorization level required by a user to perform this task is Admin.

Prerequisites

An owner should already be assigned to the sce-url-database.

Options

encryption-key—AES encryption key (128-bits long). The key is supplied in hexadecimal format and contains 32, 48, or 64 hexadecimal digits.

Default

No encryption key is configured.

Removing the Encryption Key

To remove the encryption key, use the **no sce-url-database protection encryption-key** command.

This command does not change any other sce-url-database protection settings.



Note When you change the encryption key of the sce-url-database, this message appears on the CLI: *Due to changes in security settings existing protection database is being removed.*

You can ignore the message.

How to Remove All the Protection Rules for the sce-url-database

To remove all the protection rules for the sce-url-database, use the following command in the interface linecard configuration mode (config if):

no sce-url-database protection

This command can be executed only by the assigned owner of the sce-url-database. The authorization level required by a user to perform this task is Admin.

Prerequisites

An owner should already be assigned to the sce-url-database.

Results

The following are the results for removing all the protection rules in the sce-url-database:

- Removes all protection rules for the the sce-url-database and resets the sce-url-database automatically
- Reverts to the default protection settings:
 - No designated owner user
 - No protections
 - No encryption key

How to View the Current sce-url-database Protection Settings

To view the current sce-url-database protection settings, use the use the following command in User EXEC (>) mode:
show interface linecard 0 sce-url-database protection.

The authorization level required by a user to perform this task is Viewer.

Results

The following information is displayed when the show interface linecard 0 sce-url-database protection command is run:

- Username of the owner
- Information about the current protection settings
- Information about whether encryption key is configured

3 Managing the sce-url-database

The designated owner of the sce-url-database can do perform the following tasks:

- Import the list of URLs from an sce-url-database file.
- Add a single entry to the sce-url-database.
- Clear the sce-url-database.
- Look up a specific URL (unless lookup protection is set to no-user).

If write protection is set to all-users, all the users can perform the following tasks:

- Import the list of URLs from an sce-url-database file.
- Add a single entry to the sce-url-database.
- Clear the sce-url-database.

If there is no designated owner (and therefore, no protection), all the users can view the entire sce-url-database.

If there is a designated owner, the contents of the sce-url-database are protected and cannot be displayed.

Guidelines for Managing the sce-url-database

The guidelines for managing the sce-url-database include:

- When a new file is imported, the existing database is cleared before the import. Because incremental update is not supported, the import file must contain all the relevant URLs, not just the new ones to be added to the database.
- Import operation ensures zero downtime for the protected URL blacklisting. The previous list of URLs remains in effect throughout the import operation. The new list of URLs comes into effect immediately after it is fully imported.
- A large number of new URLs can be added by importing an updated sce-url-database file. Typically, if the database is protected, this option is used with an encrypted file.
- New URLs can be added by using the **sce-url-database add-entry** command.

The sce-url-database Import File

The maximum number of entries permitted in an import file are:

- Cisco SCE 8000 platform—100,000
- Cisco SCE 2000 platform—100,000

The database import file either contains cleartext or is encrypted. If the file is encrypted, the matching encryption key must be configured by the database owner.

If the file is encrypted, it must be prefixed with a cleartext header. The encrypted file header must be as follows:

```
Encrypted file version: 0x01
Block cipher index: 0x01
Mode of operation index: 0x02
Padder index: 0x02
IV length: 0x10
IV: <16 unformatted bytes which form the 128 bits IV of the encrypted data >
```

After the header, the following data appears in the encrypted format in the AES 128, CFB mode:

A random number (in the range [16...31]) of random bytes, followed by the word "Signed", and then again 32 random bytes.

Each following line represents a single URL.

The import file format of the sce-url-database is:

```
[Flavor <tab>] URL
```

Here:

- Flavor—Flavor ID. This must either be included for every line in the file or for none of the lines. The flavor must be separated from the URL by a <tab>.

- URL—(* | [*] [Host-Suffix] | [*] [Host-Suffix] / [URL-Prefix [*]] [URL suffix] [? Params-prefix])

Table 1 lists some URL examples.

Table 1 **Defining URLs**

URL Input	Look Up Table (LUT) Key Output	Result
*	*.*.*.*	Blocks all URLs.
*.com	*.com:.*.*	Blocks all the URLs in which the host ends with .com.
*/media	*./media:.*.*	Blocks all the URLs in which the path contains only media.
*/media*mp3	*./media*.*mp3:*	Blocks all the URLs in which the path starts with media and ends with mp3.
*/?*key	*/*.*.*key*	Blocks all the URLs in which the parameters start with key.
*.com/media*mp4?download	*.com:/media*.*mp4:download*	Blocks all the URLs in which: <ul style="list-style-type: none"> • The host ends with .com. • The path starts with media and ends with mp4. • The parameters start with download.

How to Import a sce-url-database File

See the “[The sce-url-database Import File](#)” section on page 7 for information about the sce-url-database import file format.

To import the sce-url-database files, use the following command in the interface linecard configuration mode (config if):

sce-url-database import cleartext-file | encrypted-file *file-name* **flavor-id** *flavor-id*

If the import file does not contain a flavor, specify the flavor in the CLI. The specified flavor must be the same as the one that was designated for the blacklist in the PQB file that was applied. Otherwise the import operation fails.

If the import file contains a flavor, do not specify the flavor in the CLI.

The authorization level required by a user to perform this task is Admin.

Prerequisites

The user executing the command must have write permission to the sce-url-database.

Options

The following options are available to import a sce-url-database file:

- **cleartext-file**
- **encrypted-file**—An encrypted file can be imported only if a matching encryption key has been configured.
- **file-name**—The Path and filename of the sce-url-database import file.
- **flavor-id**—The flavor that is applied to all the entries in the file.

Default

The sce-url-database is empty.

Results

The following are the results after importing a sce-url-database file:

- The sce-url-database is cleared.
- The entries from the file are written to the database.
- The duplicate keys in the file are overwritten with no warning.
- If failure occurs while an entry is being written, the writing continues with the subsequent entries.

The total number of failures and a listing of the failed file line numbers are reported after the import action is completed.

- If the sce-url-database import file has a problem (for example, the file does not contain a flavor ID), the import procedure stops and does not proceed further. This may also result in an empty LUT.

For example:

```
SCE8000(config if)#> do show int 1 0 sce-url num-entries
14 entries found
SCE8000(config if)#> <k:vk@64.103.125.217/c:/NirTemp/enc/URLONLY2E.CSV
Error - Line 1 can not be parsed. Flavor-id is not found, it wasn't supplied through CLI
Error - Operation aborted.
SCE8000(config if)#> do show int 1 0 sce-url num-entries
No entries found
```

How to Add an Entry to the sce-url-database

To add an entry to the sce-url-database, use the following command in the interface linecard configuration mode (config if):

sce-url-database add-entry url-wildcard *URL-wildcard-format* **flavor-id** *flavor-id*

The authorization level required by a user to perform this task is Admin.

Prerequisites

The user who is executing the command must have write permission to the sce-url-database.

Options

The following options are available to add an entry to the sce-url database:

- *URL-wildcard-format*—
URL: (* | [*] [Host-Suffix] | [*] [Host-Suffix] / [URL-Prefix [*]] [URL suffix] [? Params-prefix])
See [Table 1](#) for examples on how to define URLs.
- *flavor-id*—Decimal number representing the flavor. It is required when adding a single entry.

How to View the sce-url-database

To view the sce-url-database, use the following command in the Privileged EXEC (#) mode:

show interface linecard 0 sce-url-database all-entries

The authorization level required by a user to perform this task is Admin.

Prerequisites

All protection must be removed from the sce-url-database and there should be no assigned owner. If an assigned owner exists, the database becomes protected and cannot be displayed.

How to Look for a Specific URL in the sce-url-database

To look for a specific URL in the sce-url-database, use the following command in the Privileged EXEC (#) mode:

show interface linecard 0 sce-url-database url *url*

The authorization level required by a user to perform this task is Admin.

Prerequisites

The user who is executing the command must have lookup permission in the sce-url-database.

Options

url—Specific URL to look up in the sce-url-database.

Results

The following are the results when the user tries to look for a specific URL in the sce-url-database file:

- If the specified URL exists, the flavor index is returned.
- If you are trying to look up a URL in a database for which you are not the owner, you will receive a message that the URL does not exist even if it does.

How to Clear the sce-url-database

To clear the sce-url-database, use the following command in the interface linecard configuration mode (config if):

sce-url-database remove-all

The authorization level required by a user to perform this task is Admin.


Prerequisites

The user executing the command must have write permission in the sce-url-database.

4 Enabling Deep HTTP Inspection

The HTTP flows may contain multiple transactions. Typically, each such inner URL should be verified against the protected URL database, not just the initial one. However, because this has a deep impact on performance HTTP inspection is disabled by default.

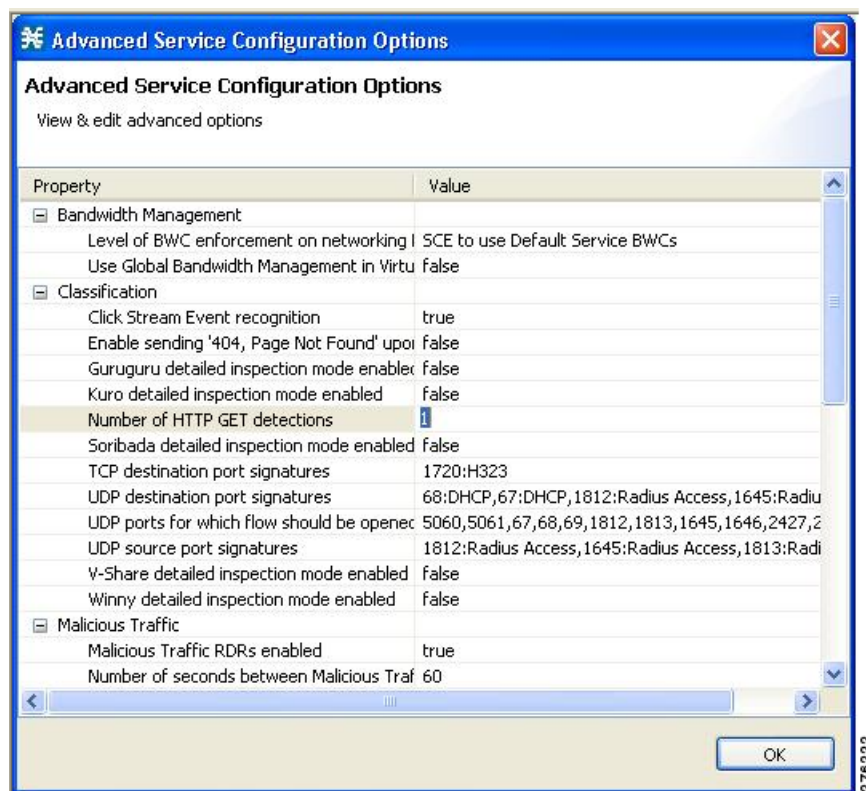
You can enable the deep HTTP inspection option from the Cisco SCA BB Console. The actual configuration relates to the number of HTTP transactions that are examined per HTTP flow (number of HTTP GET detections). By default, only the first transaction is examined; you can define this to be any number of transactions between 1 and 65535.

 **Note** We recommend that you monitor the performance of the Cisco SCE platform when deep HTTP inspection is enabled, because enabling this functionality may result in performance degradation.

How to Enable Deep HTTP Inspection

Step 1 In the SCA BB Console Service Configuration Editor, choose
Configuration > System Settings > Advanced Options tab > Advanced Service Configuration Options.

Figure 1 Advanced Service Configuration Options Window



Step 2 In the Advance Services Configuration Options window that is displayed (Figure 1), in the **Number of HTTP GET** detections field, enter the number of HTTP transactions to examine the per HTTP flow. The valid value ranges from 1 to 65535.

5 URL Normalization

URL normalization is a procedure that brings URL flavors having the same meaning into a canonical presentation, which minimizes the number of false-negative lookup results and may significantly improve the efficiency of the protected blacklisting operation.

URL normalization involves the following:

- Percent-encoding
- Case sensitivity

By default, these normalization operations are disabled, but when enabling URL normalization, both of them come into effect for the protected blacklist.

You must first enable URL normalization and then import the blacklist entries so that they are affected accordingly.

Configuring URL Normalization

Use the URL normalization commands to:

- Globally enable URL normalization.
- Globally disable URL normalization (default).
- Set URL normalization to the default state (disabled).
- Display the current configured state of URL normalization.

URL normalization should be configured before service configuration (PQB file) is applied to the Cisco SCE platform and before the sce-url-database is loaded.

How to Enable URL Normalization

To enable the URL normalization, use the following command in the interface linecard configuration mode (config if):

lookup canonical

The authorization level required by a user to perform this task is Root.

How to Disable URL Normalization

To disable the URL normalization, use the following command in the interface linecard configuration mode (config if):

no lookup canonical

The authorization level required by a user to perform this task is Root.

How to Reset URL Normalization to the Default State

To reset the URL normalization to the default state, use the following command in the interface linecard configuration mode (config if):

no lookup canonical

By default, the URL normalization is disabled. The authorization level required by a user to perform this task is Root.

How to Display the Currently URL Normalization Configuration

To display the current URL normalization configuration, use the following command in the User EXEC (>) mode:

show applications slot 0 lookup canonical

The authorization level required by a user to perform this task is Viewer.

6 Protected URL Database Configuration Example

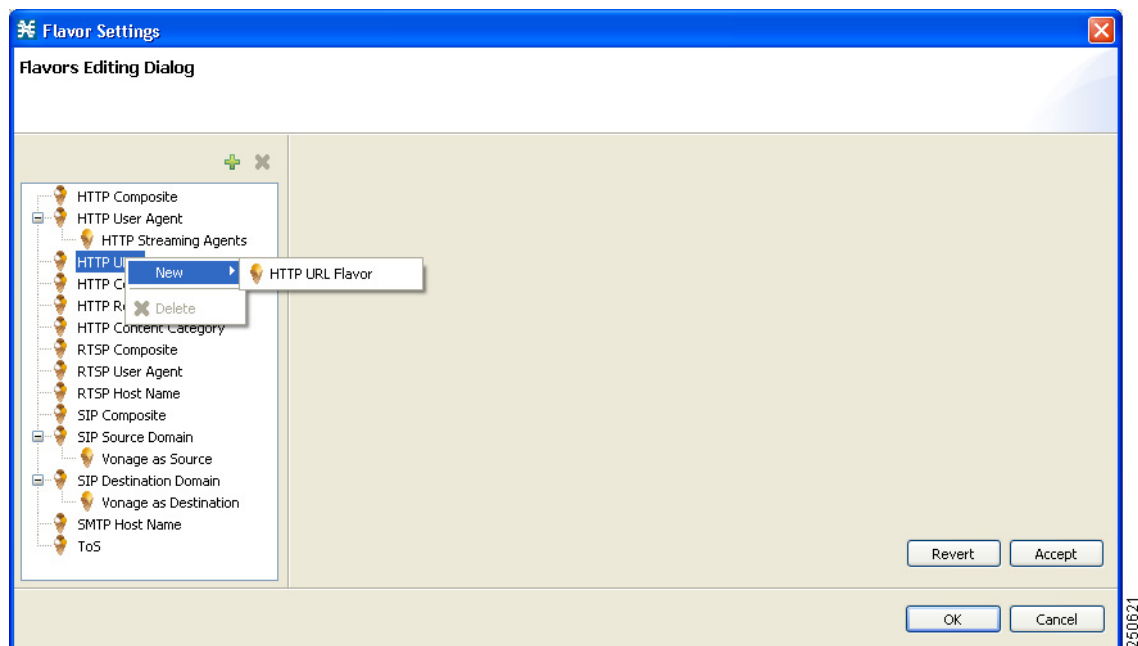
The following example shows how to configure the protected URL database, including defining the flavors in the Cisco SCA BB Console, configuring the protections in the Cisco SCE platform, and importing a URL file.

Step 1 Enable URL normalization as shown here:

```
> enable 15
#> configure
(config)#> interface LineCard 0
(config if)#> lookup canonical
```

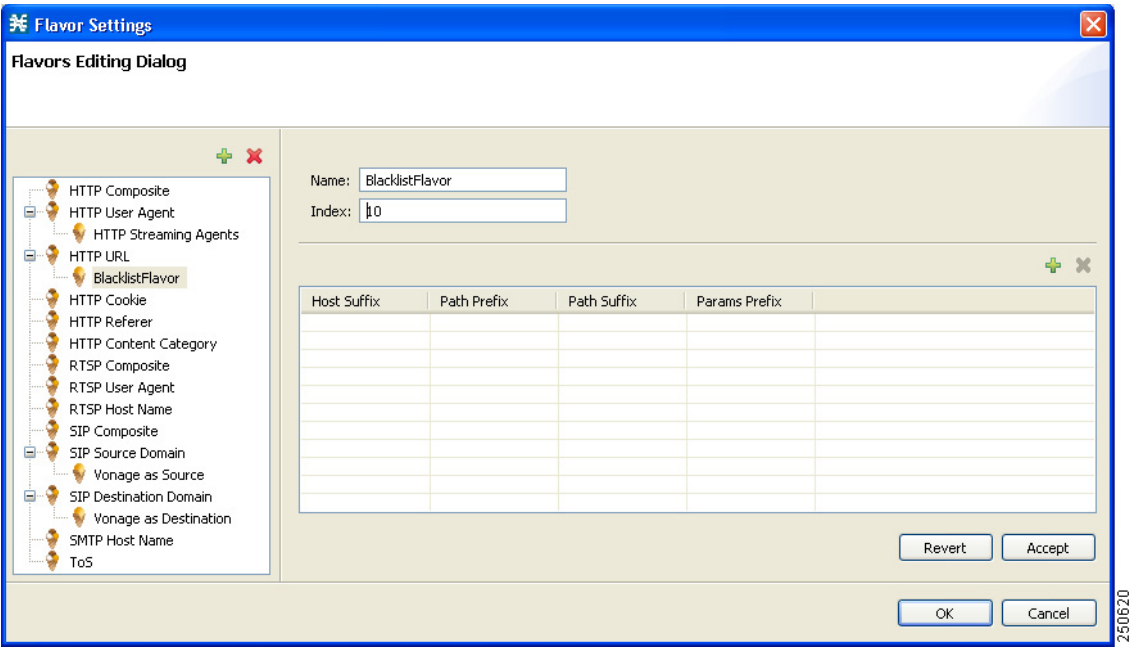
Step 2 In the Flavor Settings window, right-click HTTP URL and choose New > HTTP URL Flavor (see [Figure 2](#)).

Figure 2 Flavor Settings—Flavors Editing Dialog Box



Step 3 Enter a Name and Index, as required (see [Figure 3](#)).The Index number is the flavor ID that is required by a number of CLI commands.

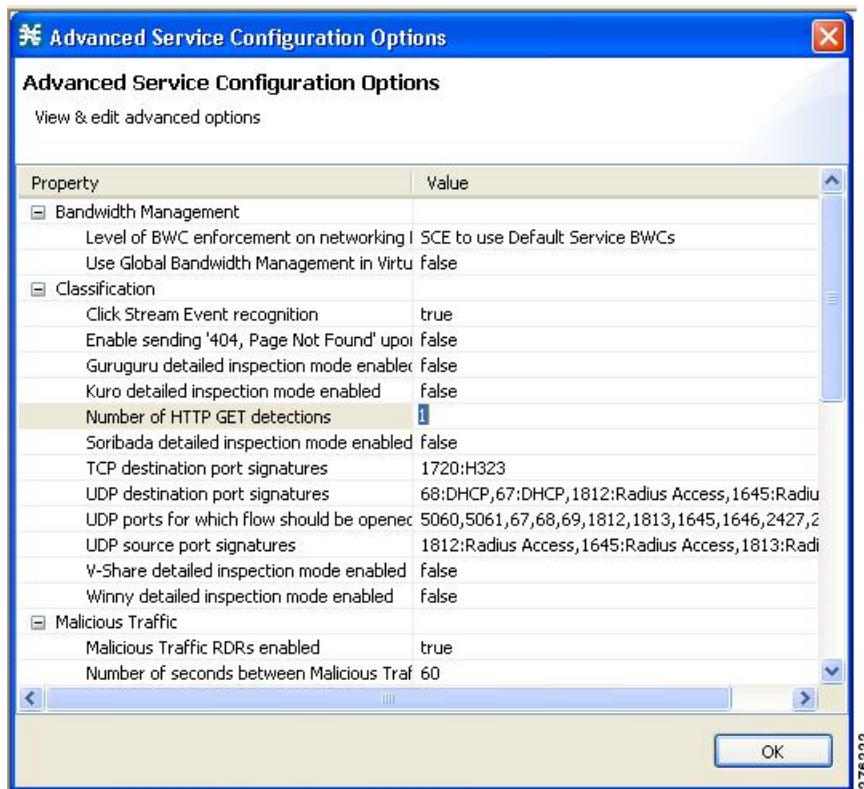
Figure 3 Flavor Settings—Flavors Editing Dialog Box with Name and Index Information



- Step 4** Click OK.
- Step 5** Define a service that will use the new flavor.

Step 6 Specify the number of HTTP GET detections.

Figure 4 *Advanced Service Configuration Options Window*



Step 7 In the Service Configuration Editor window, choose Configuration > System Settings > Advanced Options tab > Advanced Service Configuration Options. The Advanced Service Configuration Options window opens (see Figure 4).

Step 8 In the Advance Services Configuration Options window, in the Number of HTTP GET detections field, enter the number of HTTP transactions to examine per HTTP flow (1 to 65535).

Step 9 Apply the service configuration to the Cisco SCE.

Step 10 Define the Cisco SCE to require user login and define the special owner user using the `username BlacklistOwner privilege 10 password pass` command as shown in the following example:

```
# configure
(config)# aaa authentication login default local enable none
(config)# username BlacklistOwner privilege 10 password pass
```

Step 11 Log in as the owner using the following information:

```
User Access Verification
Username: BlacklistOwner
Password:
```

Step 12 Configure the owner of the sce-url-database using the `sce-url-database protection owner myself` command, as shown in the following example:

```
# configure
(config)# interface LineCard 0
(config if)# sce-url-database protection owner myself
```

Step 13 (Optional) Allow all the users to update the database using the `sce-url-database protection allow-write all-users` command, as shown in the following example:

```
(config if)# sce-url-database protection allow-write all-users
```

Step 14 (Optional) Provide the owner with the necessary permission to perform the lookup action on the database using the **sce-url-database protection allow-lookup owner-only** command, as shown in the following example:

```
(config if)# sce-url-database protection allow-lookup owner-only
```

Step 15 Define an encryption key to be used when importing an encrypted URLs file using the **sce-url-database protection encryption-key** command, as shown in the following example:

This should be done periodically over a secure Telnet session.

```
(config if)# sce-url-database protection encryption-key AABCCDDEEFF11223344556677889900
```

Step 16 Import an encrypted file containing the required URLs for the relevant flavor ID using the **sce-url-database import encrypted-file urls.csv flavor-id** command, as shown in the following example:

```
(config if)# sce-url-database import encrypted-file urls.csv flavor-id 10
```

This should be done periodically; either by copying the file to Cisco SCE first or by importing directly over FTP.

Step 17 Save the configuration using the **copy running-config-all startup-config-all** command, as shown in the following example:

```
(config if)#> exit
(config)#> exit
#> copy running-config-all startup-config-all
Writing general configuration file to temporary location...
Backing-up general configuration file...
Copy temporary file to final location...
Writing general (protected) configuration file to temporary location...
Backing-up general (protected) configuration file...
Copy temporary (protected) file to final location...
Writing general configuration file to temporary location...
Removing old application configuration file...
Renaming temporary application configuration file with the final file's name...
Writing general (protected) configuration file to temporary location...
Removing old application (protected) configuration file...
Renaming temporary application (protected) configuration file with the final file's name...
```

Step 18 Log out to prevent unauthorized users from manipulating the protected database using the **logout** command, as shown in the following example:

```
# logout
```

7 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2011-2012 Cisco Systems, Inc. All rights reserved.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.