CHAPTER 16

Electronic Surveillance Server

Revised: July 24, 2009, OL-3743-42

The Electronic Surveillance Server (ess) table holds the information related to the Delivery Function (DF) server and is populated at system installation.

Table Name: ESS

Table Containment Area: EMS, Call Agent, and FSPTC

Command Types

Show, add, change, and delete

Examples

```
show ess cdc-df-address=191.12.301.211; cdc-df-port=1813;
add ess cdc-df-address=191.12.301.211; cdc-df-port=1813; encryption-key=0000000000000000;
protocol-version=I03;
change ess cdc-df-address=191.12.301.211; cdc-df-port=1813;
acc-req-retransmit=4;acc-rsp-timeout=3;
delete ess cdc-df-address=191.12.301.211; cdc-df-port=1813;
```

Usage Guidelines

Primary Key Token(s): cdc-df-address, cdc-df-port

Add Rules: None.

Change Rules: None.

Delete Rules: None.

IPSec Rules:

- ipcsec-sa-lifetime must be greater than or equal to 0.
- ipsec-sa-grace-period must be greater than or equal to 0.
- ipsec-sa-grace-period must less than or equal to 25% of ipsec-sa-lifetime.
- ike-group: the list must contain 1, but other possible lists are: <1>, or <1, 2>.
- ike-sa-lifetime must be greater than or equal to 0.
- ike-key-encr must be stored in an encrypted format.

Note An asterisk preceding a token name means the token is mandatory. A token without an asterisk is optional.

Syntax Description

* CDC-DF-ADDRESS	Primary key. Identifies the DNS or IP address of the DF server to send the call data and call content. VARCHAR(64): 1–64 ASCII characters.
* PROTOCOL-VERSION	Specifies the PacketCable event message (EM) version. VARCHAR(8): 1–8 ASCII characters. Permitted values are: I02—Encodes the EM headers with 60 bytes. I03—(Default) EM-I03 and up. Encodes EM headers with 76 bytes.
ACC-REQ-RETRANSMIT	Specifies the number of retransmissions of unacknowledged accounting requests. INTEGER: 1–4 (Default = 3).
ACC-RSP-TIMEOUT	Time (in seconds) to retransmit the radius message. The value must be an integer. INTEGER: Default = 2.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
CDC-DF-PORT	Primary key. Identifies the port number of the DF server to send the call data packets. INTEGER: 0–65535 (Default = 1813).
DESCRIPTION	Described by the service provider. VARCHAR(64): 1–64 ASCII characters.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
ENCRYPTION-KEY	MD5 Encryption Key for the radius interface between the Cisco BTS 10200 Softswitch and the DF server. VARCHAR(16): 1–16 ASCII characters (Default = 0000000000000000).

IKE-CS	Specifies a list of ciphersuites supported by IKE, in priority order. This list is used to negotiate the encryption-authentication algorithm pair used by IKE. The list can contain only those ciphersuites using the authentication algorithms HMAC-MD5 and HMAC-SHA and the encryption algorithm ESP-3DES. VARCHAR(64): 1–64 ASCII characters. Permitted values are: 3DES-MD5, 3DES-SHA1 (Default list) 3DES-SHA1, 3DES-MD5 3DES-MD5 3DES-SHA1
IKE-GROUP	Identifies the available groups in which the Diffie-Helman exchange can occur. INTEGER: Valid values are 1 and 2 (Default = 2).
IKE-KEY	The IKE preshared key. An ike-key value must be provisioned for a trunking gateway, and is optional for other gateways. VARCHAR(512): 1–512 ASCII characters.
IKE-KEY-ENCR	The IKE preshared key in encrypted form (system generated). The system encrypts the value of the IKE-KEY token and stores the encrypted value as IKE-KEY-ENCR. It is then decrypted and displayed only when accessed by a privileged user. VARCHAR(256): 1–256 ASCII characters. To show the ike-key-encr token in encrypted form, use the following command: show radius-profile; To show the ike-key token in unencrypted form, use the following command: show radius-profile-unencr;
IKE-SA-LIFETIME	Specifies the IKE SA expiration, in seconds. INTEGER: 0–MAXINT (Default = 86400). **Note** MAXINT is defined as the largest possible 4-byte integer, that is, [2 to the power 32]–1.
IPSEC-CMS-CONTROL-PORT	IPSec SA outbound control port. Used if the SA is created for a particular outbound port for this device class. SMALLINT: 0–65534 (Default = 0).

IPSEC-SA-ESP-CS	The IPSec SA ESP ciphersuite list in priority order. Used to negotiate an encryption-authentication algorithm pair used by IPSec. The list can contain only those ciphersuites using the authentication algorithms HMAC-MD5 and HMAC-SHA and the encryption algorithms ESP-3DES and ESP-NULL. VARCHAR(64): 1–64 ASCII characters. 3DES-MD5, 3DES-SHA1, NULL-MD5, NULL-SHA1 (Default list) **Note** This list can be modified to be a subset of this initial list using the CLI and can be reordered to specify a new priority selection. For example: - 3DES-MD5, 3DES-SHA1, NULL-SHA1, NULL-MD5 - 3DES-SHA1, NULL-MD5, NULL-SHA1 - 3DES-MD5, NULL-MD5 - NULL-SHA1 and additional values
IPSEC-SA-GRACE-PERIOD	Sets the IPSec SA key expiration grace period, in seconds. This is used to calculate the soft expiration. The ipsec-sa-grace-period must be less than the ipsec-sa-lifetime. INTEGER: 0–MAXINT (Default = 3600). **Note** MAXINT is defined as the largest possible 4-byte integer, that is, [2 to the power 32]–1. **Note** The value of ipsec-sa-grace-period must be less than or equal to 25% of the provisioned value for ipsec-sa-lifetime. If not specified when provisioning a new ipsec-sa-lifetime, the ipsec-sa-grace-period defaults to 25% of the ipsec-sa-lifetime.
IPSEC-SA-LIFETIME	Sets the IPSec SA expiration, in seconds. This is the hard expiration. INTEGER: 0–MAXINT (Default = 86400). **Note** MAXINT is defined as the largest possible 4-byte integer, that is, [2 to the power 32]–1.
IPSEC-ULP-NAME	Specifies a single IPSec SA upper-layer protocol. Use this token if the SA should be created only for specific protocol traffic for this device class. VARCHAR(8): 1–8 ASCII characters. The value is a string as described in getprotobyname(3XNET). Permitted values are: IP (Default) TCP UDP
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.

ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).
USE-PACKETCABLE-IAP	Specifies whether to use IAP for PacketCable. Set this flag to N if the Cisco BTS 10200 Softswitch does not need to search for a PacketCable CALEA enabled IAP for CALEA Call Content (SII only). This flag is typically set to N in a network with no available PacketCable-compliant Intercept Access Points (IAPs). CHAR(1): Y/N (Default = N). Y—PacketCable IAPs are searched for call content. N—PacketCable IAPs are not searched for call content. The Cisco BTS 10200 Softswitch assumes the DF server knows where to send the wiretap request using SDP information.