CHAPTER 4

CWMP Technology Commands

This chapter contains information about the command line interface (CLI) commands that you can use to manage and monitor the CPE WAN Management Protocol (CWMP) technology on the Broadband Access Center (BAC) Device Provisioning Engine (DPE).

Using the commands described in this chapter, you can configure settings for the CWMP services and the HTTP file services on the DPE. Both services feature individual instances: service 1 and service 2, each of which you must configure separately.

BAC supports different instances so that you can configure different options for each service. For example, CWMP service 1 is, by default, configured to require HTTP digest authentication; but without supporting HTTP over SSL/TLS. This service is configured to run on port 7547 and is enabled by default. CWMP service 2 is configured on port 7547 with HTTP over SSL/TLS; but is disabled by default. You can reconfigure any of these defaults for each service to suit your requirements. See Table 4-1 for the default configuration for each service.

Table 4-1 Default Settings for CWMP Technology

	CWMP Service		HTTP File Service	
	Service 1	**Service 2**	**Service 1**	**Service 2**
Mode	Enabled	Disabled	Enabled	Disabled
Authentication	Digest	Digest	Digest	Digest
Port Number	7547	7548	7549	7550
HTTP over SSL/TLS	Disabled	Enabled	Disabled	Enabled

Note You cannot globally enable or disable CWMP-related services. You can enable or disable CWMP features only individually.

The commands described in this chapter are:

service cwmp

This is the global syntax of the commands that you can use to configure various settings for the CWMP service running on the DPE. Using these commands, you can:

- Enable the CWMP service
- Specify the instance of the service,
- Configure client authentication and client certificate authentication
- Set the port number for the service
- Configure the service to use HTTP over SSL/TLS.

Use **service cwmp** in conjunction with the commands listed in Table 4-2.

Note When using these commands, you must restart the DPE—unless specified otherwise—for the changes to take effect. To restart the DPE, run the **dpe reload** command (see dpe reload, page 3-5).

Table 4-2 List of service cwmp Commands

Command Usage	Syntax Description	Examples
service cwmp *num* allow-unknown-cpe **no service cwmp *num* allow-unknown-cpe**		
Enables or disables the DPE to request configuration from the RDU for devices unknown to the DPE. **Note** Enabling this feature may allow a Denial of Service attack on the RDU. You need not restart the DPE for this command to take effect.	*num*—Identifies the CWMP service, which could be 1 or 2.	`dpe# service cwmp 1 allow-unknown-cpe` `% OK`

Table 4-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* client-auth *mode*		
Enables or disables client authentication for the CWMP service on the DPE. For a list of authentication options in BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.	• *num*—Identifies the CWMP service, which could be 1 or 2. • *mode*—Identifies the client authentication mode for the CWMP service. The client authentication mode could be: – **basic**—Enables Basic HTTP authentication. – **digest**—Enables Digest HTTP authentication. This is the default configuration. – **none**—Disables Basic and Digest authentication. In this mode, the CWMP service uses the Device ID in the Inform message to authenticate CPE. **Note** To limit security risks during client authentication, Cisco recommends using the Digest mode (the default configuration). It is not advisable to allow client authentication in the Basic mode, or altogether disable Basic and Digest authentication.	`dpe# service cwmp 1 client-auth digest` `% OK (Digest authentication was enabled. Basic authentication was disabled. Requires DPE restart "# dpe reload")`
service cwmp *num* enable {true | false}		
Enables or disables the CWMP service running on the DPE.	• *num*—Identifies the CWMP service, which could be 1 or 2. By default, the CWMP service is: – Enabled on service 1. – Disabled on service 2. • **true**—Enables the CWMP service. • **false**—Disables the CWMP service.	`dpe# service cwmp 2 enable true` `% OK (Requires DPE restart "# dpe reload")`
service cwmp *num* port *port*		
Identifies the port on which the CWMP service communicates with the CPE. By specifying a different port number, this command enables the DPE to prevent potential sharing violations among ports used by other applications.	• *num*—Identifies the CWMP service, which could be 1 or 2. • *port*—Identifies the port number that is to be used by the service. By default, the CWMP service is configured to listen on: – Port 7547 for service 1. – Port 7548 for service 2.	`dpe# service cwmp 1 port 7547` `% OK (Requires DPE restart "# dpe reload")`

Table 4-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp session timeout *value*		
Sets the duration for timing out a CWMP session. **Note** You need not restart the DPE for this command to take effect.	*value*—Identifies the timeout period for the CWMP session, in milliseconds (ms). The timeout period could be anything between 1000 ms (1 second) and 3000000 ms (50 minutes). By default, the duration for a timeout is set as 60000 ms (60 seconds).	`dpe# service cwmp session timeout 60000` `% OK`
service cwmp *num* external-url *url*		
Configures the DPE to represent externally the specified URL as the URL of the CWMP service.	• *num*—Identifies the CWMP service, which could be 1 or 2. • *url*—Identifies the URL that is to be used for the CWMP service.	`dpe# service cwmp 1 external-url https://192.0.2.1:7547/acs` `% OK`

Table 4-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl client-auth *mode*		

Enables or disables client certificate authentication using HTTP over SSL/TLS for the CWMP service running on the DPE.
 	
For a list of authentication options in BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.
	• *num*—Identifies the CWMP service, which could be 1 or 2.
	
	By default, client certificate authentication with SSL/TLS is:
	– Disabled for service 1.
	– Disabled for service 2.
	• *mode*—Identifies the mode of client certificate authentication for the CWMP service. BAC supports:
	– **client-cert-generic**—Enables client certificate authentication through SSL/TLS by using a generic certificate common to all CPE or a large subset of CPE. The client certificate is validated by using the signing certificate authority's public key. This key is preconfigured in the DPE keystore. This certificate-validation process ensures that the certificate is valid, but does not establish the identity of a device. Therefore, the device identifier is not formed by using the data in the CN field of the client certificate. Instead, the device identifier is formed by using the data provided via Basic or Digest authentication, or by using the data in the CWMP Inform message.
	– **client-cert-unique**—Enables client certificate authentication through SSL/TLS by using the unique certificate that each CPE provides. After the client certificate is validated by using the signing certificate authority's public key, the device's unique identifier is formed by using the CN field of the client certificate.
	– **none**—Disables client certificate authentication by using HTTP over SSL/TLS for the CWMP service.
		Example 1
		`dpe# service cwmp 1 ssl client-auth client-cert-generic`
		`% OK (Requires DPE restart "# dpe reload")`
		
		Example 2
		`dpe# service cwmp 1 ssl client-auth client-cert-unique`
		`% OK (Requires DPE restart "# dpe reload")`

Table 4-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl client-auth client-cert-ext		
Enables the authentication of CPE whose connection that used HTTP over SSL/TLS was terminated at a Load Balancer (Cisco ACE 4710). The ACE extracts information about the SSL session, specifically client certificate fields, from the CPE and inserts that data into various HTTP headers. BAC then retrieves the CN field from the header ClientCert-Subject-CN to form the unique device identifier. **Note** Before enabling this command, ensure that you configure ACE to insert the client certificate fields into the HTTP header. For a list of authentication options in BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.	*num*—Identifies the CWMP service, which could be 1 or 2. By default, client certificate authentication by using HTTP over SSL/TLS for the CWMP service is: • Disabled for service 1. • Disabled for service 2.	`dpe# service cwmp ssl 1 client-auth client-cert-ext` `% OK (Requires DPE restart "# dpe reload")`

Table 4-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl cipher {all-cipher-suites | *value*} **no service cwmp *num* ssl cipher {all-cipher-suites | *value*}**		

Enables or disables authentication between the DPE server and CPE by using cryptographic algorithms, or ciphers, supported by HTTP over SSL/TLS for certificate management and session management. During an SSL handshake, the DPE server and a CPE identify the strongest cipher suite enabled on both, and use that suite for the SSL session.
 	
Note BAC supports a list of cipher suites that you can configure from the DPE command line interface. For a list of cipher suites supported in BAC, see Table 4-6.
	• *num*—Identifies the CWMP service, which could be 1 or 2.
	
	• **all-cipher-suites**—Enables all the cipher suites to authenticate a session by using HTTP over SSL/TLS for the CWMP service. This is the default configuration.
	
	Note The **service cwmp ssl cipher all-cipher-suites** command works only if you have not configured any individual ciphers. To disable an individual cipher suite, use the **no service cwmp ssl cipher** *value* command. To disable all ciphers, use the **no service cwmp ssl cipher all-cipher-suites** command.
	
	• *value*—Identifies the individual cipher to be enabled for authenticating a session by using HTTP over SSL/TLS for the CWMP service. You can enable or disable any cipher suite.
	
	Each cipher suite specifies a set of algorithms that are associated with a specific cryptography function. For a list of cryptography algorithms supported in BAC, see Table 4-5.
		Example 1
		`dpe# service cwmp 1 ssl cipher all-cipher-suites`
		`% OK (Requires DPE restart "# dpe reload")`
		
		Example 2
		`dpe# service cwmp 1 ssl cipher ssl_dh_anon_with_des_cbc_sha`
		`% OK (Requires DPE restart "# dpe reload")`

Table 4-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl enable {true | false}		
Enables or disables use of HTTP over SSL/TLS for the CWMP service on the DPE. **Note** The CWMP service will fail to start up if you do not configure the keystore file and the keystore passwords before restarting the DPE. For information on how to configure a keystore file and keystore passwords, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.	• *num*—Identifies the CWMP service, which could be 1 or 2. • **true**—Enables SSL/TLS transport. This is the default configuration for service 2. • **false**—Disables SSL/TLS transport. This is the default configuration for service 1.	`dpe# service cwmp 1 ssl enable true` `% OK (Requires DPE restart "# dpe reload")`

Table 4-2 List of service cwmp Commands (continued)

Command Usage	Syntax Description	Examples
service cwmp *num* ssl keystore *keystore-filename keystore-password key-password*		
Sets a keystore file, which contains the provisioning server certificate. This certificate is used to authenticate the provisioning server to the devices by using HTTP over SSL/TLS. **Note** This setting is relevant only if the service instance is enabled (as in the case of **service cwmp 2**, which is by default disabled), and the SSL/TLS protocol is enabled for that service. To enable SSL/TLS transport, use the **service cwmp *num* ssl enable true** command.	• *num*—Identifies the CWMP service, which could be 1 or 2. • *keystore-filename*—Identifies the keystore file that you created previously. • *keystore-password*—Identifies the keystore password that you used when you created your keystore file. The keystore password must be between 6 and 30 characters. • *key-password*—Identifies the private key password that you used when you created your keystore file. The private key password must be between 6 and 30 characters.	`dpe# service cwmp 1 ssl keystore example.keystore changeme changeme` `% OK (Requires DPE restart "# dpe reload")`
The DPE ships with a default sample keystore, which contains a self-signed certificate. However, because a CWMP device does not trust a self-signed certificate, you cannot use this keystore to enable HTTP over SSL/TLS to provision a device; instead, you must obtain a signed service provider certificate and keystore. For detailed information, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.		

service cwmp-redirect

This is the global syntax of the commands that you can use to configure various settings for the cwmp-redirect service running on the DPE. Using these commands, you can:

- Enable the cwmp-redirect service.
- Configure the number of attempts and retry timeout for querying other provisioning groups.
- Configure the maximum number of devices that the DPE queries for every second.
- Set the status period for sending status request queries.
- View the statistics of cwmp-redirect service running on the DPE.

Use **service cwmp-redirect** in conjunction with the commands listed in Table 4-3

Table 4-3 List of service cwmp-redirect commands

Command Usage	Syntax Description	Examples
service cwmp-redirect 1 lookup enabled {true | false}		
Enables or disables the DPE to send home provisioning group queries to other provisioning groups when a device is unknown. If a provisioning group responds that the device belongs to its group, the device is redirected to that provisioning group. You must specify an interface for provisioning group communication before you run this command. See interface ip pg-communication, page 3-7. You need not restart the DPE for this command to take effect.	• **true**—Enables the DPE to send home provisioning group queries to other provisioning groups when a device is unknown. • **false**—Prevents the DPE from sending home provisioning group queries to other provisioning groups when a device is unknown.	`dpe# service cwmp-redirect 1 lookup enabled true` `% OK`
service cwmp-redirect 1 respond enabled {true | false}		
Enables or disables the DPE to respond to the home provisioning group queries sent from other provisioning groups. You must specify an interface for provisioning group communication before you run this command. See interface ip pg-communication, page 3-7. You need not restart the DPE for this command to take effect.	• **true**—Enables the DPE to respond to the home provisioning group queries sent from other provisioning groups • **false**—Prevents the DPE from responding to the home provisioning group queries sent from other provisioning groups.	`dpe# service cwmp-redirect 1 lookup respond enabled true` `% OK`

Table 4-3 List of service cwmp-redirect commands (continued)

Command Usage	Syntax Description	Examples
service cwmp-redirect 1 timeout *value*		
Sets the duration for which the DPE waits for a response from the other provisioning groups, after sending a home provisioning group query. You need not restart the DPE for this command to take effect.	*value*—Specifies the duration for which the DPE waits for a response from the other provisioning groups. It must be equal to or greater than 50 milliseconds.	dpe# **service cwmp-redirect 1 timeout 100** % OK
service cwmp-redirect 1 attempts *value*		
Sets the maximum number of attempts made by the DPE to send the home provisioning group queries to the other provisioning groups. You need not restart the DPE for this command to take effect.	*value*—Specifies the maximum number of attempts made by the DPE to send the home provisioning group queries to other provisioning groups. It must be equal to or greater than 1.	dpe# **service cwmp-redirect 1 attempts 3** % OK
service cwmp-redirect 1 limit *value*		
Sets the maximum number of devices that the DPE queries for every second to locate the home provisioning group of the device. You need not restart the DPE for this command to take effect.	*value*—Specifies the maximum number of devices that the DPE queries for every second. It must be equal to or greater than 1.	dpe# **service cwmp-redirect 1 limit 50** % OK
service cwmp-redirect 1 status-period *value*		
Specifies the duration at which the DPE sends status request queries to the DPEs in other provisioning groups. You need not restart the DPE for this command to take effect.	*value*—Specifies the duration at which the DPE sends status request queries to other provisioning groups. It must be equal to or greater than 50 milliseconds.	dpe# **service cwmp-redirect 1 status-period 2500** % OK
service cwmp-redirect 1 retry-after-timeout *value*		
Specifies the timeout after which the DPE informs the device to retry later, if the DPE is not able to establish communication with other DPEs due to some error or the home provisioning group of the device cannot be found. You need not restart the DPE for this command to take effect.	*value*—Specifies the timeout after which the DPE informs the device to retry later, if the home provisioning group of the device cannot be found. It must be equal to or greater than 1000 milliseconds.	dpe# **service cwmp-redirect 1 retry-after-timeout 2500** % OK

show service cwmp-redirect 1 statistics

Displays the statistics of the home provisioning group redirection service running on the DPE.

Syntax Description No keywords or arguments

Examples

```
dpe# show service cwmp-redirect 1 statistics
PG            DPE              State      Status RQ/RP    Lookup RQ/RP
Los Angeles   10.86.147.122    Sync       2/1             0/0
Boston        192.168.0.27     Down       15903/0         0/0
New York      192.168.0.2      Down       15903/0         0/0
Chicago       192.168.0.12     Down       15903/0         0/0
```

The output presented in this example is trimmed.

keystore import-pkcs12

Use this command to import existing private key and certificates into a DPE-compatible file used in authenticating the DPE to SSL clients. The **keystore import-pkcs12** command opens a PKCS#12 file, reads the contents, and writes a new keystore in the Sun-proprietary Java keystore format called JKS.

The PKCS#12 file format is a standard used for storing certificates and private keys; for example, an imported certificate from a Microsoft Windows 2000 IIS 5.0 server.

Note If your private key and certificate are stored in separate files, combine them into a single PKCS#12 file before running the **keystore import-pkcs12** command.
You can use the syntax described in the following example, where the **openssl** command combines the keys in `example.key` and the certificate in the `example.crt file` into the `example.pkcs12` file:
`#` **openssl pkcs12 -inkey example.key -in example.crt -export -out example.pkcs12**

Syntax Description **keystore import-pkcs12** *keystore-filename pkcs12-filename keystore-password* key-password *export-password export-key-password*

- *keystore-filename*—Identifies the JKS keystore file that will be created. If it already exists, it will be overwritten.

  Note Remember to specify the full path of the keystore file.

- *pkcs12-filename*—Identifies the PKCS#12 file from which you intend to import the key and certificate.
- *keystore-password*—Identifies the private key password and the keystore password that you used when you created your keystore file. This password must be between 6 and 30 characters.
- *key-password*—Identifies the password used to access keys within DPE keystore. This password must be between 6 and 30 characters.

- *export-password*—Identifies the password used to decrypt the key in the PKCS#12 file. The export password must be between 6 and 30 characters.
- *export-key-password*—Identifies the password used to access keys within the PKCS#12 keystore. This password must be between 6 and 30 characters.

Examples

```
dpe# keystore import-pkcs12 example.keystore example.pkcs12 changeme changeme changeme
changeme
% Reading alias [1]

 % Reading alias [1]: key with format [PKCS8] algorithm [RSA]

 % Reading alias [1]: cert type [X.509]

 % Created JKS keystore: example.keystore

 % OK
```

service http

This is the global syntax of the commands that you use to configure various settings for the HTTP service running on the DPE. Using these commands, you can:

- Enable the service
- Specify the instance of the service
- Configure client authentication and client certificate authentication
- Set the port number for the service
- Configure the service to use HTTP over SSL/TLS

Use **service http** in conjunction with the list of commands described in Table 4-4.

Note When using these commands, you must restart the DPE—unless specified otherwise—for the changes to take effect. To restart the DPE, run the **dpe reload** command (see dpe reload, page 3-5).

Table 4-4 List of service http Commands

Command Usage	Syntax Description	Examples
service http *num* client-auth *mode*		
Enables or disables client authentication for the HTTP file service on the DPE. For a list of authentication options in BAC, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*	• *num*—Identifies the HTTP file service, which could be 1 or 2. • *mode*—Identifies the client authentication mode for the HTTP file service. The client authentication mode could be: – **basic**—Enables Basic HTTP file service authentication. – **digest**—Enables Digest HTTP file service authentication. This is the default configuration. – **none**—Disables Basic and Digest authentication. In this mode, the HTTP file service uses the Device ID in the Inform message to authenticate CPE. **Note** To limit security risks during client authentication, Cisco recommends using the Digest mode (the default configuration). It is not advisable to allow client authentication in the Basic mode, or disable Basic and Digest authentication.	`dpe# service http 1 client-auth digest` `% OK (Digest authentication was enabled. Basic authentication was disabled. Requires DPE restart "# dpe reload")`

Table 4-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* enable {true | false}		
Enables or disables the HTTP file service running on the DPE	• *num*—Identifies the HTTP file service, which could be 1 or 2. By default the HTTP file service is: – Enabled on service 1. – Disabled on service 2. • **true**—Enables the HTTP file service. • **false**—Disables the HTTP file service.	`dpe# service http 2 enable true` `% OK (Requires DPE restart "# dpe reload")`
service http *num* port *port*		
Identifies the port on which the HTTP file service communicates with a CPE device. By specifying a different port number, this command enables the DPE to prevent potential sharing violations among ports used by other applications.	• *num*—Identifies the HTTP file service, which could be 1 or 2. By default, the HTTP file service is configured to listen on: – Port 7549 for service 1. – Port 7550 for service 2. • *port*—Identifies the port number that is to be used by the service. **Note** The **service http port** command does not check if the port number specified is being used by other applications or system utilities.	`dpe# service http 1 port 7549` `% OK (Requires DPE restart "# dpe reload")`
service http *num* external-url *url*		
Configures the DPE to represent externally the specified URL as the URL of the HTTP file service.	• *num*—Identifies the HTTP file service, which could be 1 or 2. • *url*—Identifies the URL that is to be used for the HTTP file service.	`dpe# service http 1 external-url https://192.0.2.27:7547 /acs` `% OK`

Table 4-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl client-auth *mode*		

Enables or disables client certificate authentication by using HTTP over SSL/TLS for the HTTP file service running on the DPE.
 	
For a list of authentication options in BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.
	• *num*—Identifies the HTTP file service, which could be 1 or 2.
	
	By default, client certificate authentication by using HTTP over SSL/TLS for the HTTP file service is:
	– Disabled for service 1.
	– Disabled for service 2.
	• *mode*—Identifies the mode of client certificate authentication for the HTTP file service. BAC supports:
	– **client-cert-generic**—Enables client certificate authentication through SSL/TLS by using a generic certificate common to all CPE or a large subset of CPE. The public key of the signing certificate authority is used to validate the client certificate. This key is preconfigured in the DPE keystore. This certificate validation process ensures that the certificate is valid, but does not establish identity of a given device. Therefore, the device identifier is not formed by using the data in the CN field of the client certificate. Instead, the device identifier is formed by using the data provided via Basic or Digest authentication, or by using the data in the CWMP Inform message.
	– **client-cert-unique**—Enables client certificate authentication through SSL/TLS using the unique certificate provided by each CPE. After the client certificate is validated by using the signing certificate authority's public key, the device's unique identifier is formed by using the CN field of the client certificate.
	– **none**—Disables client certificate authentication by using HTTP over SSL/TLS.
		Example 1
		`dpe# service http 1 ssl client-auth client-cert-generic`
		`% OK (Requires DPE restart "# dpe reload")`
		
		Example 2
		`dpe# service http 1 ssl client-auth client-cert-unique`
		`% OK (Requires DPE restart "# dpe reload")`

Table 4-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl client-auth client-cert-ext		
Enables the authentication of CPE whose connection that uses HTTP over SSL/TLS was terminated at a Load Balancer (Cisco ACE 4710). The ACE extracts information about the SSL session, specifically client certificate fields, from the CPE, and inserts that data into various HTTP headers. BAC then retrieves the CN field from the header ClientCert-Subject-CN to form the unique device identifier. **Note** Before you enable this command, ensure that you configure ACE to insert the client certificate fields into the HTTP header. For a list of authentication options in BAC, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.	*num*—Identifies the HTTP file service, which could be 1 or 2. By default, client certificate authentication that use HTTP over SSL/TLS for the HTTP file service is: • Disabled for service 1. • Disabled for service 2.	dpe# **service http ssl 1 client-auth client-cert-ext** % OK (Requires DPE restart "# dpe reload")

Table 4-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl cipher {all-cipher-suites | *value*} **no service http *num* ssl cipher {all-cipher-suites | *value*}**		

Enables or disables authentication between the DPE server and CPE by using cryptographic algorithms, or ciphers, that HTTP supports over SSL/TLS for certificate management and session management. During an SSL handshake, the DPE server and a CPE device identify the strongest cipher suite enabled on both, and use that suite for the SSL session.
 	
Note BAC supports a list of cipher suites that you can configure from the DPE command line interface. For a list of cipher suites that BAC supports, see Table 4-6.
	• *num*—Identifies the HTTP file service, which could be 1 or 2.
	
	• **all-cipher-suites**—Enables all the cipher suites to authenticate a session by using HTTP over SSL/TLS for the HTTP file service. This is the default configuration.
	
	Note The **service http ssl cipher all-cipher-suites** command works only if you have not configured any individual ciphers. To remove an individual cipher suite, use the **no service http ssl cipher** *value* command. To disable all ciphers, use the **no service http ssl cipher all-cipher-suites** command.
	
	• *value*—Identifies the individual cipher to be enabled for authenticating a session using HTTP over SSL/TLS for the HTTP file service. You can enable or disable any cipher suite.
	
	Each cipher suite specifies a set of algorithms that are associated with a specific cryptography function. For a list of cryptography algorithms that BAC supports, see Table 4-5.
		Example 1
		`dpe# service http 1 ssl cipher all-cipher-suites`
		`% OK (Requires DPE restart "# dpe reload")`
		
		Example 2
		`dpe# service http 1 ssl cipher ssl_dh_anon_with_des_cbc_sha`
		`% OK (Requires DPE restart "# dpe reload")`

Table 4-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl enable {true | false}		
Enables or disables use of HTTP over SSL/TLS for the HTTP file service on the DPE. **Note** The HTTP file service will fail to start up if you do not configure the keystore file and the the keystore passwords before restarting the DPE. For information on how to configure a keystore file and keystore passwords, refer to the *Cisco Broadband Access Center Administrator's Guide, Release 3.5.*	• *num*—Identifies the HTTP file service, which could be 1 or 2. • **true**—Enables SSL/TLS transport. This is the default configuration for service 2. • **false**—Disables SSL/TLS transport. This is the default configuration for service 1.	`dpe# service http 1 ssl enable true` `% OK (Requires DPE restart "# dpe reload")`

Table 4-4 List of service http Commands (continued)

Command Usage	Syntax Description	Examples
service http *num* ssl keystore *keystore-filename keystore-password key-pasword*		
Sets a keystore file, which contains the provisioning server certificate. This certificate is used to authenticate the provisioning server to the devices by using HTTP over SSL/TLS. **Note** This setting is only relevant if the service instance is enabled (as in the case of service http 2, which is by default disabled) and HTTP over SSL/TLS is enabled for the service. To enable SSL/TLS transport, use the **service http num ssl enable true** command.	• *num*—Identifies the HTTP file service, which could be 1 or 2. • *keystore-filename*—Identifies the keystore file that you created previously. • *keystore-password*—Identifies the keystore password that you used when you created your keystore file. The keystore password must be between 6 and 30 characters. • *key-password*—Identifies the private key password that you used when you created your keystore file. The private key password must be between 6 and 30 characters.	`dpe# service http 1 ssl keystore example.keystore changeme changeme` `% OK (Requires DPE restart "# dpe reload")`

The DPE ships with a default sample keystore, which contains a self-signed certificate. However, because a CWMP device does not trust a self-signed certificate, you cannot use this keystore to enable HTTP over SSL/TLS to provision a device; instead, you must obtain a signed service provider certificate and keystore.

For detailed information on how to obtain a signed service provider certificate and keystore, see the *Cisco Broadband Access Center Administrator's Guide, Release 3.5*.

Selecting Cipher Suites

A typical SSL session requires encryption ciphers to establish and maintain the secure connection. Cipher suites provide the cryptographic algorithms that the SSL/TLS protocol requires to authenticate client/server exchanges, and establish and maintain secure connections.

Table 4-5 defines the cryptography algorithms supported in this release of BAC:

Table 4-5 Cryptography Algorithms Supported in BAC

Cryptography Function	Algorithms Supported in BAC
SSL versions	SSL version 3.0 and Transport Layer Security (TLS) version 1.0
Public key exchange and key agreement algorithms	• RSA (key exchange and key agreement algorithm) The Rivest, Shamir, and Adelman algorithm used for encryption and digital signatures. - 512-bit, 768-bit, 1024-bit, and 2048-bit • DSA (certificate signing algorithm) The Digital Signature Algorithm used as part of the Digital Signature Standard (DSS). - 512-bit, 768-bit, and 1024-bit • Diffie-Hellman (key exchange algorithm) - 512-bit, 768-bit, 1024-bit, and 2048-bit
Encryption types	• DES The Data Encryption Standard applies a 56-bit key to each 64-bit block of data. This key is used for encryption and decryption. • 3DES or Triple DES The Triple-Strength Data Encryption Standard in case DES is used with three keys. • RC4 The Rivest Cipher 4 which is a variable key-size stream cipher used for file encryption.
Message authentication algorithms	• MD5 (Message Digest 5) The algorithm used in digital signature applications to produce a 128-bit message digest, which is unique to the message and can be used to verify data integrity. • Secure Hash Algorithm (SHA) The algorithm used in the Digital Signature Standard to produce a 160-bit hash value.

Caution The dh-anon series of cipher suites are intended for completely anonymous Diffie-Hellman communications in which neither party is authenticated. Note that this cipher suite is vulnerable to attacks.

Cipher suites with “export” in the title indicate that they are intended for use outside the United States. These cipher suites have encryption algorithms with limited key sizes, for example, 3DES or RC4 with 128-bit encryption.

Table 4-6 Cipher Suites Supported in BAC

Cipher Suite	Exportable	Key Exchange Algorithm Used
all-cipher-suites	No	EDH *
ssl_dh_anon_export_with_des40_cbc_sha	Yes	DH **
ssl_dh_anon_with_des_cbc_sha	No	DH **
ssl_dh_anon_export_with_rc4_40_md5	Yes	DH **
ssl_dh_anon_with_3des_ede_cbc_sha	No	DH **
ssl_dhe_dss_with_des_cbc_sha	No	DH **
ssl_dh_anon_with_rc4_128_md5	No	DH **
ssl_dhe_dss_export_with_des40_cbc_sha	Yes	EDH *
ssl_dhe_dss_with_3des_ede_cbc_sha	No	EDH *
ssl_dhe_rsa_export_with_des40_cbc_sha	Yes	EDH *
ssl_dhe_rsa_with_3des_ede_cbc_sha	No	EDH *
ssl_dhe_rsa_with_des_cbc_sha	No	EDH *
ssl_rsa_export_with_des40_cbc_sha	Yes	RSA
ssl_rsa_export_with_rc4_40_md5	Yes	RSA
ssl_rsa_with_3des_ede_cbc_sha	No	RSA
ssl_rsa_with_des_cbc_sha	No	RSA
ssl_rsa_with_null_md5	No	RSA
ssl_rsa_with_null_sha	No	RSA
ssl_rsa_with_rc4_128_md5	No	RSA
ssl_rsa_with_rc4_128_sha	No	RSA
tls_dh_anon_with_aes_128_cbc_sha	No	DH **
tls_dhe_dss_with_aes_128_cbc_sha	No	EDH *
tls_dhe_rsa_with_aes_128_cbc_sha	No	EDH *
tls_rsa_with_aes_128_cbc_sha	No	RSA

* refers to the Ephemeral Diffie-Hellman algorithm
** refers to the Diffie-Hellman algorithm.