Symantec™ Managed PKI for SSL VICE2 Web Services Developer's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Contents

Chapter 1

Overview of VICE 2 web services and this guide

This chapter includes the following topics:

About this guide

This guide is intended to help developers integrate your SSL certificate applications with VICE 2.0 web services. To use VICE 2.0 web services, you should understand the following concepts:

- HTTP (Hypertext Transfer Protocol)
- SSL (Secure Sockets Layer)
- Web services

Introduction

The web services-based Virtual Interface for Certificate Enrollment (VICE) 2.0 for Managed PKI for SSL enables your organization to provide automated SSL certificate lifecycle services for enrollment, pickup, renewal, revocation, and retrieval of available units and, if you choose, set up automatic approval of SSL certificates so that they are issued instantly.

VICE 2.0 web services

VICE 2.0 provides Representational State Transfer (REST) style web services running on top of HTTPS, with client authentication.

VICE 2.0 supports the acquisition of the following types of Managed PKI for SSL server certificates:

Premium SSL	All of the features of Standard SSL, plus server-gated cryptography (SGC), which is suited to older browsers, and regularly scheduled vulnerability assessments.
Standard SSL	SSL certificate-based security, with verification of your business identity and domain ownership, plus website mailware scans, the Secured Seal, and Seal-in-Search.
Premium Extended Validation (EV) SSL	All of the features of Standard EV, plus SGC.
Standard Extended Validation (EV) SSL	The EV standard requires a CA to adopt a specific certificate validation practice and pass a Webtrust audit. To indicate the presence of an EV SSL certificate, high security web browsers have visual cues. For instance, some internet browsers show a green address bar, the organization in the certificate, and the certificate's security vendor.
Premium Intranet SSL	Premium SSL for an intranet or private network.
Standard Intranet SSL	Standard SSL for use on an intranet or private network.
OFX SSL	Authenticates and secures commerce on the internet.

For more information on the server certificates issued through Managed PKI for SSL, see the *Symantec Managed PKI for SSL Administrator's Guide*.

Enabling your account to integrate with VICE 2.0 web services

To make use of the VICE 2.0 web services, you must add web services to your account.

To enable your account to integrate with the VICE 2.0 web services

1. Contact Symantec Customer Service or your sales representative to request the VICE 2.0 web services feature for your account. Symantec Customer Service activates the feature for your account.
2. After the web services feature is activated for your account, enroll for an additional Managed PKI for SSL administrator ID and request a special Web Services role for this administrator ID. Your SSL certificate application needs to import the Web Services administrator ID as the client certificate to access VICE 2.0 web services.
3. Optionally you can enable **Automatic Approval** for your SSL certificates enrolled through the VICE 2.0 web services. Your Configuration Administrator can enable this option ("Enable Auto Issuing for Enrollment through Web Services") in the Managed PKI for SSL Control Center enrollment configuration wizard. Once enabled your SSL certificate enrollments through the VICE 2.0 web services are instantly issued without approval from your administrators.

Testing your SSL certificate application

You can test your SSL certificate application in our pilot environment. To do so, you'll need to create a test account. Creating a test account allows you to test in our pilot environment without affecting your regular account. The test account provides free test units to use in your test API calls. After creating a test account, use your test account credentials and the pilot endpoints in your certificate API requests.

To get a test account and certificate units, email enterprise-sslsupport@symantec.com.

VICE 2.0 transactions

A VICE 2.0 transaction (consisting of a request and response) is an interaction between your SSL certificate application and the VICE 2.0 web services. VICE 2.0 supports the following types of transactions:

Enrollment	With an enrollment transaction, your SSL certificate application sends an enrollment request to VICE 2.0 and receives a response containing the certificate status information, transaction ID, and optionally the base-64 encoded certificate if the certificate is enrolled successfully and automatically approved.
Pickup	With a pickup transaction, your SSL certificate application sends a pickup request with the transaction ID to VICE 2.0 and receives a response containing the certificate status information and the base-64 encoded certificate when the certificate is approved (automatically or manually by your Administrators).
Renewal	With a renewal transaction, your SSL certificate application sends a renewal request to VICE 2.0 and receives a response containing the certificate status information, transaction ID, and optionally the base-64 encoded certificate if the certificate is renewed successfully and automatically approved.
Revocation	With a revocation transaction, your SSL certificate application sends a certificate revocation request to VICE 2.0 and receives a response containing the revocation status information.
Approve	The approve transaction allows your application to approve SSL certificate orders. With an approve transaction, your SSL certificate application sends an approval request to VICE 2.0 and receives a response containing the certificate information.
Reject	The reject transaction allows your application to reject SSL certificate orders. With an reject transaction, your SSL certificate application sends a reject request to VICE 2.0 and receives a response containing a confirmation of the order rejection.
Token Availability	With a token availability transaction, your SSL certificate application sends a token availability request to VICE 2.0 and receives a response containing the number of available certificate units for each certificate product type in your account.

Note: If you run out of certificate units, your certificate enrollment and renewal requests cannot be approved. Contact your Symantec sales representative to purchase additional certificate units.

Customer support

For additional information regarding VICE 2.0 web services, certificate enrollment, and Managed PKI for SSL in general:

- Review our support Knowledge Base at https://knowledge.verisign.com/.
- Visit our website at https://knowledge.verisign.com/support/mpki-for-ssl-support.
- Email enterprise-sslsupport@symantec.com.

Chapter 2

Message format structure

This chapter includes the following topics:

Overview of message format structure

This chapter describes the basic message format structure for all VICE 2.0 requests and responses.

Request format

The Managed PKI for SSL Web Services use REST style message format over HTTP. Only the GET and POST request methods are supported. All other methods sent in the request will result in unsupported protocol errors.

GET method

When using the GET method, use this request format:

```
GET <WebServiceURL>?<urlencoded name=value parameters> HTTP/1.0
```

POST method

When using the POST method, use this request format:

```
POST <WebServiceURL> HTTP/1.0
Content-Type: application/x-www-form-urlencode
Content-Length: <length of the encoded body>

<url encoded parameters>
```

The POST method requires the Content-Type and Content-Length headers. All other headers are optional.

The Content-Type and Content-Length headers must have the following settings:

- Set Content-Type to application/x-www-form-urlencoded.
- Set Content-Length to match the exact length of the urlencoded body.

See the remaining chapters in this book for the service endpoints and request parameters. Use the ampersand character (&) to separate parameters.

Note: For the GET and POST methods, using HTTP/1.1 is optional. VICE 2.0 enforces HTTP/1.0 but not HTTP/1.1.

You can use the optional Date and User-Agent header fields for system tracking.

Response format

After the service successfully connects with the client request, it sends a response back to the client. An HTTP response code of 200 indicates that the service was able to process the request and the client should continue to parse the response message to determine the transaction status. All other HTTP response codes indicate a problem with the request or connection. Table 2-1 is a list of all possible HTTP response codes.

Table 2-1 HTTP response codes

Response code	Description
200	OK
400	Bad Request
401	Unauthorized
403	Forbidden

Table 2-1 HTTP response codes *(continued)*

Response code	Description
404	Not found
405	Method Not Allowed
408	Request Timeout
500	Internal Server Error
503	Service Unavailable

For valid 200 HTTP responses, the content-type will be text/xml. The response message block will be in XML or JSON (for reporting services).

Caution: Your application should not use string pattern matching to parse responses, as the response may include additional information or attributes in future releases. Use an XML parser for XML responses and a JSON parser for reporting service responses.

Depending on whether the transaction is successful, two types of response messages are returned:

Success response:

```
<Response xmlns="urn:symantec:api">
<StatusCode>[Status Code]</StatusCode>
<Message>Description</Message>
[Additional Info]...
</Response>
```

Failure response:

```
<Error xmlns="urn:symantec:api">
<StatusCode>[Status Code]</StatusCode>
<Message>Description</Message>
</Error>
```

Note: The status code in the XML response is a hexadecimal Symantec Managed PKI for SSL status code.

Chapter 3

Enrolling for an SSL certificate

This chapter includes the following topics:

Overview of enrolling for an SSL certificate

This chapter includes detailed request and response information for certificate enrollment transactions.

Request (enrollment)

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/enroll

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/enroll

Table 3-1 lists the parameters that can be sent through an Enrollment transaction. Some parameters are required.

Table 3-1 Enrollment request parameters

Name	Data type	Required	Max Length	Description
challenge	Text	Y	32	Challenge phrase for the certificate.
firstName	Text	Y	240	Subscriber first name.
middleInitial	Text	N	1	Subscriber middle initial.
lastName	Text	Y	240	Subscriber last name.
email	Text (e-mail address)	Y	240	Subscriber email address. You can enter multiple email addresses separated by comma.
csr	Base64 encoded CSR	Y		The base-64 encoded PKCS#10 certificate request for the Enrollment transaction. The headers ("-----BEGIN..." and "-----END...") are optional. To generate a CSR, use your server software. When you generate the CSR, for certificates that expire after November 1, 2015 you must supply the common name in the form of a fully qualified domain name (FQDN).
certProductType	Certificate type parameter	Y		Certificate product type. See Table 3-2 on page 18.
serverType	Server type parameter	Y		Server software type. See one of the following: ■ Table 3-3 ■ Table 3-4 ■ Table 3-5

Table 3-1 Enrollment request parameters *(continued)*

Name	Data type	Required	Max Length	Description
validityPeriod	1Y, 2Y, or 3Y	Y	2	Validity period.
specificEndDate	MM/DD/YYYY	N	10	The end date for the certificate. The end date must be less than 2 years from the validity start date for EV certificates, and less than 3 years from the validity start date for other certificates. For this parameter to take effect, you must enable an option the Control Center. Go to the **Configuration** tab, **Enrollment** page, **Select Certificate Lifecycle Options** section, and select **Applicants can request a specific end date within the validity period**.
extraLicenses	Number (0-999)	N	3	Extra number of licenses to bind with the certificate. The default value is 0.
comment	T61	N	512	Subscriber comments.
jobTitle	T61	N	64	Subscriber title.
employeeID	T61	N	64	Subscriber employee ID number.
serverIP	Text	N	15	Server IP address.
mailStop	T61	N	64	Subscriber mailstop.
signatureAlgorithm	Text (see Description field)	N		The certificate's signature algorithm. Enter one of the following values: ■ `sha1WithRSAEncryption` ■ `sha256WithRSAEncryption` ■ `DSAwithSHA256` ■ `ECDSAwithSHA256` If you do not specify the signature algorithm and the CSR contains an RSA key, `sha1WithRSAEncryption` is the default.
ctLogOption	Text (see Description field)	N		Determines whether the EV certificate information will be stored in Certificate Transparency public logs permanently. The default value is public. Enter one of the following values: ■ `public` ■ `nolog`

Table 3-1 Enrollment request parameters *(continued)*

Name	Data type	Required	Max Length	Description
additionalField#	T61	N	64	Enter up to 10 additional fields. # indicates 1-10.
subject_alt_name#	Text (valid FQDN)	N	255	The subject alternative names (SANs). One certificate can secure the common name in the CSR and additional domains that are entered as SANs (also known as subjectAltName). Each SAN must be an FQDN. Enter up to 100 SANs. # indicates 1-100.
subject_alt_names	Text	N		A comma-separated list of domain names. Enter up to 100 SANs. Example: mail.symantec.com, blog.symantec.com, ftp.symantec.com **Note:** You can use either subject_alt_name# (the older format, where # indicates 1-100) or the new subject_alt_names format.

Supported certificate product types

Managed PKI for SSL allows a single account to issue multiple types of SSL certificates. VICE 2.0 requirements for issuing a particular certificate type depend on your account settings and Symantec authentication policies.

Certificate product type values

The following certificate product types are supported in VICE 2.0 enrollment and renewal web services:

Note: You cannot use VICE 2.0 web services for Authenticode code signing certificates. Use the Managed PKI for SSL enrollment forms to request them and manage them using the Control Center.

Table 3-2 certProductType values

Certificate product type	VICE 2.0 certProductType value
Standard Extended Validation SSL	HAServer
Premium Extended Validation SSL	HAGlobalServer
Standard SSL	Server

Table 3-2 certProductType values *(continued)*

Certificate product type	VICE 2.0 certProductType value
Premium SSL	GlobalServer
Standard Intranet SSL	IntranetServer
Premium Intranet SSL	IntranetGlobalServer
Private SSL	PrivateServer
Rapid SSL Enterprise	GeotrustServer
Private SSL	PrivateServer

Certificate validation criteria

VICE 2.0 supports enrollment, issuance, and renewal for all certificate types (with the exception of Authenticode code signing). To manage activities for a particular certificate type through VICE 2.0, your Managed PKI for SSL account must meet the following requirements:

- Your must be able to issue and manage the particular certificate product type through your Subscriber Services pages and the Managed PKI for SSL Control Center.
- You must have enabled the particular certificate type for subscribers in the Managed PKI for SSL Control Center (using the Enrollment Wizard).
- For OFX SSL Certificates, Symantec must approve your account to issue OFX certificates.
- For Standard and Premium Extended Validation (EV) SSL certificates, Symantec must approve your account to issue EV SSL certificates.

Supported serverType values for Standard SSL certificates

If your VICE 2.0 enrollment or renewal transaction involves an SSL certificate (SSL ID) for Managed PKI for SSL, Managed PKI for Intranet SSL, or Extended Validation see Table 3-3 to provide a value for the serverType parameter. This list includes serverType values for Standard EV SSL, Standard SSL, and Standard Intranet SSL certificates.

Note: Corresponding certProductType values are HAServer, Server, and IntranetServer, respectively.

Table 3-3 serverType values for Standard EV SSL, Standard SSL, and Standard Intranet SSL certificates

Supported serverType values		
Advanced Businesslink	Intel	Red Hat
AliBaba (WarpGroup)	Internet Factory	r3
AOL/Navisoft	iPlanet	Radnet
Apache	Iserver	Roxen
Aventail	JavaSoft	SilverStream Software
BEA WebLogic	Lotus	Sirius Software
Backweb	Marimba	Sonic WALL
Beyond Software	Microsoft	Sterling Software
Brokat	Microsoft FrontPage 98	Stronghold (C2Net)
C2Net Apache SSL-US	Microsoft Visual InterDev 6.0	Tandem
Cacheflow	Mirapoint	Tektonic
Compaq	Mitem	Tempest Software
Consensus	Nanoteq	Tenon (WebTen)
Control Data Systems	NetCentric	Thawte Consulting
Covalent	Netscape	Unify
Dascom	Netscreen	Unisys
Domino	Novell	Unwired Planet
F5	Nokia	Velocity Software
Frontier Technologies	Nortel Networks (Alteon)	Volera

Table 3-3 serverType values for Standard EV SSL, Standard SSL, and Standard Intranet SSL certificates *(continued)*

Supported serverType values		
Gradient	OpenConnect Systems	Wall Data
Hummingbird	Open Market	WebMethods
IBM	Oracle	WebSphere
I/NET	O'Reilly & Associates	WebSTAR
Information Builders	Process Software	Zeus
Information Hyperlink	Purveyor	
Ingrian Networks	Quarterdeck/StarNine	

Supported serverType values for Premium SSL certificates

If your VICE 2.0 enrollment or renewal transaction involves a Premium EV SSL, Premium SSL, or Premium Intranet SSL certificate, see Table 3-4 to provide a value for the serverType parameter.

Note: Corresponding certProductType values are HAGlobalServer, GlobalServer, and IntranetGlobalServer, respectively.

Table 3-4 serverType values for Premium EV SSL, Premium SSL, and Premium Intranet SSL certificates

serverType value		
Advanced Businesslink	IBM HTTP	Nokia
AOLServer w/ nsopenssl	Ingrian Networks	Nortel Networks (Alteon)
Apache	Intel	Novell
Aventail	iPlanet	O'Reilly WebSite 2.5 (or higher)

Table 3-4 serverType values for Premium EV SSL, Premium SSL, and Premium Intranet SSL certificates *(continued)*

serverType value		
BEA WebLogic	Lotus	Red Hat
C2Net Stronghold	Microsoft	Silver Stream
Cacheflow	Microsoft FrontPage 98	Sonic WALL
Compaq	Microsoft Visual InterDev 6.0	Tandem
Covalent	Mirapoint	Velocity Software
Domino	Nanoteq	WebMethods
F5	Netscape	WebSphere
Hummingbird	Netscreen	Zeus

Supported serverType values for OFX SSL certificates

If your VICE 2.0 enrollment or renewal transaction involves an OFX SSL certificate, see Table 3-5 to provide a value for the serverType parameter.

Note: The corresponding certProductType value is OFXServer.

Table 3-5 serverType values for OFX SSL certificates

serverType value
Microsoft
Netscape

Supported serverType values for Private SSL certificates

If your VICE 2.0 enrollment or renewal transaction involves a Private SSL certificate, see Table 3-6 to provide a value for the serverType parameter.

Note: The corresponding certProductType value is PrivateServer.

Table 3-6 serverType values for Private SSL certificates

serverType value
Microsoft
Other

Sample request

The following is a sample enrollment request using the POST method:

```
POST https://certmanager-webservices.websecurity.symantec
.com/vswebservices/rest/services/enroll HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 1301

additionalField7=7&firstName=ws&additionalField6=6&additionalField5=5&co
mment=mpki4ssl+web+services+enrollment&additionalField4=4&additionalFiel
d3=3&additionalField2=2&additionalField1=1&certProductType=GlobalServer&
employeeID=eid1234&subject_alt_name4=san20.symantec.com&subject_alt_name
3=san19.symantec.com&subject_alt_name2=san2.symantec.com&subject_alt_nam
e1=san1.symantec.com&csr=-----BEGIN+NEW+CERTIFICATE+REQUEST-----%0AMIIBp
DCCAQ0CAQAwZDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWEx%0AFjAUBgNVBA
cTDU1vdW50YWluIFZpZXcxDjAMBgNVBAoTBW1jZWxwMRgwFgYDVQQD%0AEw93cy52ZXJpc2l
nbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMiT%0AIGXTdLji%2BJZ4pKLHFF
TB%2BQyyWSduAiz0cvLd36wxH%2B3gYDzknbiaVg81jFdyRQTt%0A7ZWvLswQ1F75GGyWaLs
278lltGDMvp06HrA3wrKiCokAfW6PXjnBCkEwmS3kiD1H%0AgavyBHAhnhzFhmmqrYDZ9dX0
qq2aFkLXi1pnUbn%2FAgMBAAGgADANBgkqhkiG9w0B%0AAQsFAAOBgQBnRMeUafT%2F9nKhB
l4BNEYAuolkFvk%2Bpn7su15Wp0X4kiXJD0JiZu%2BL%0Ait7WjtPenwpVCNYEJsxqUn66ec
lJ0jtxZZKcj%2Bl7uZUl2eJl%2FAjypb3LBiGiSTR4%0AjhNiJJ%2Fea3SELjc0QS%2F7wlJ
fOVE%2B%2FAP7mTUhQywzwgXhfMPjUI4%2BNg%3D%3D%0A-----END+NEW+CERTIFICATE+R
EQUEST-----%0A%0A&serverType=Microsoft&additionalField10=10&deptNo=dept1
00&lastName=test&email=foo%40symantec.com&validityPeriod=1Y&additionalFi
eld9=9&challenge=p&jobTitle=engineer&serverIP=12.34.56.78&additionalFiel
d8=8
```

Sample response

After the request is submitted, the service sends an HTTP response to the requesting application. The following is a sample of a successful enrollment transaction response:

```
HTTP/1.0 200 OK
Date: Tue, 27 Jan 2009 18:07:07 GMT
Server: Apache/2.0.63
Connection: Close
Content-Type: application/xml;charset=UTF-8
Content-Length: 2815

<Response xmlns:tns="http://webservices.mpki4ssl.symantec.com"
xmlns="urn:symantec:api">
<StatusCode>0x00</StatusCode>
<Message>success</Message>
<Certificate>
-----BEGIN CERTIFICATE-----
MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCBJYwggP/oAMC
AQICEAHylxIQ0fJuHI7ThGImWccwDQYJKoZIhvcNAQEFBQAwgboxHzAdBgNVBAoT
FlZlcmlTaWduIFRydXN0IE5ldHdvcmsxFzAVBgNVBAsTDlZlcmlTaWduLCBJbmMu
MTMwMQYDVQQLEypWZXJpU2lnbiBJbnRlcm5hdGlvbmFsIFNlcnZlciBDQSAtIENs
YXNzIDMxSTBHBgNVBAsTQHd3dy52ZXJpc2lnbi5jb20vQ1BTIEluY29ycC5ieSBS
ZWYuIExJQUJJTElUWSBMVEQuKGMpOTcgVmVyaVNpZ24wHhcNMDkwMTIzMDAwMDAw
WhcNMTAwMTIzMjM1OTU5WjBkMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZv
cm5pYTEWMBQGA1UEBxQNTW91bnRhaW4gVmlldzEOMAwGA1UEChQFbWNlbHAxGDAW
BgNVBAMUD3dzLnZlcmlzaWduLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAyJMgZdN0uOL4lnikoscUVMH5DLJZJ24CLPRy8t3frDEf7eBgPOSduJpWDzWM
V3JFBO3tla8uzBDUXvkYbJZouzbvyWW0YMy+nToesDfCsqIKiQB9bo9eOcEKQTCZ
LeSIPUeBq/IEcCGeHMWGaaqtgNn11fSqrZoWQteLWmdRuf8CAwEAAaOCAfAwggHs
MGgGA1UdEQRhMF+CEXNhbjEudmVyaXNpZ24uY29tghFzYW4yLnZlcmlzaWduLmNv
bYISc2FuMTkudmVyaXNpZ24uY29tghJzYW4yMC52ZXJpc2lnbi5jb22CD3dzLnZl
cmlzaWduLmNvbTAJBgNVHRMEAjAAMAsGA1UdDwQEAwIFoDBGBgNVHR8EPzA9MDug
OaA3hjVodHRwOi8vY3JsLnZlcmlzaWduLmNvbS9DbGFzczNJbnRlcm5hdGlvbmFs
U2VydmVyLmNybDBEBgNVHSAEPTA7MDkGC2CGSAGG+EUBBxcDMCowKAYIKwYBBQUH
AgEWHGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9ycGEwNAYDVR0lBC0wKwYJYIZI
AYb4QgQBBgorBgEEAYI3CgMDBggrBgEFBQcDAQYIKwYBBQUHAwIwNAYIKwYBBQUH
AQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wbgYI
KwYBBQUHAQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQU
S2u5KJYGDLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9nbzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4GBACHw9a71HM78FWM9PNvh8ahy
7JKaJfw1UnIqc2CgfrNBSE9EqZvum28+rT04ubaee/g9jkoyW/69hKoZxmgHMvbH
Y/YxgGPFAEe74qXrt3kILKfF80vWgtr/IqvSuhTTCnZ0tI7xk+zBpiKTLZMAKHrG
hDqbPLayiUTol1iahCslMIICdDCCAh6gAwIBAgIQLEsSHFvppgrNXe8sU4IPiDAN
BgkqhkiG9w0BAQQFADBCMQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24s
IEluYy4xGjAYBgNVBAsTEUNsYXNzIDMgVEVTVCBST09UMB4XDTk4MDEwNjAwMDAw
MFoXDTI1MDEwNjIzNTk1OVowgboxHzAdBgNVBAoTFlZlcmlTaWduIFRydXN0IE5l
dHdvcmsxFzAVBgNVBAsTDlZlcmlTaWduLCBJbmMuMTMwMQYDVQQLEypWZXJpU2ln
```

```
biBJbnRlcm5hdGlvbmFsIFNlcnZlciBDQSAtIENsYXNzIDMxSTBHBgNVBAsTQHd3
dy52ZXJpc2lnbi5jb20vQ1BTIEluY29ycC5ieSBSZWYuIExJQUJJTElUWSBMVEQu
KGMpOTcgVmVyaVNpZ24wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMlJVsro
1Div4jlqkZKSqs8Yw/jdw0+9zBYk9d9T8+sImZCJqIrDnGVPbhBJWwiPL48U6ZlQ
2ALaKLz1D1C898GYoyXuB5LnZzFWgeEV3DWTpkzDpgT6EGD0vusWQ83e+6NG6/b2
fupnMVpi1IZ6Q+RE+LsFoqoIJ7JpZIiuSYt9AgMBAAGjMzAxMBEGCWCGSAGG+EIB
AQQEAwICBDAPBgNVHRMECDAGAQH/AgEAMAsGA1UdDwQEAwIBBjANBgkqhkiG9w0B
AQQFAANBAPD3kw9bU1xRbZK+7K7SbBWNMq26iRbx9+wTAK2jpBH9WywDgC0nOrAY
R5BieNf+4BNXKEwPqUJnhymMssZuuvUAADEAAAAAAAAA
-----END CERTIFICATE-----
</Certificate>
<Transaction_ID>87d1adc3f1f262409092ec31fb09f4c7</Transaction_ID>
</Response>
```

A successful enrollment response contains a transaction ID for retrieving the certificate when it has been approved manually or automatically. If automatic approval is enabled the response will also contain a certificate for your application to extract.

Chapter 4

Picking up an SSL certificate

This chapter includes the following topics:

Overview of picking up an SSL certificate

This chapter includes detailed request and response information for certificate pickup transactions.

Request

When a certificate request is successfully entered through the VICE 2.0 Web Services, your application receives a response containing a valid transaction ID. If the certificate cannot be instantly issued because the automatic approval option is not enabled, the request appears in your Managed PKI for SSL Control Center as a pending approval request.

The request is then reviewed and approved by your Certificate Management Administrator. Once the certificate is approved, pick up the certificate with a VICE 2.0 pickup transaction. Note that your application may pick up a certificate with its transaction ID even if it is instantly issued. This allows your application to retrieve the certificate in case it gets lost.

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/pickup

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/pickup

Table 4-1 lists the certificate information that can be sent through a pickup request.

Table 4-1 Pickup request parameters

Name	Data type	Required	Max Length	Description
transaction_id	Text	Y	32	The transaction ID received during the enrollment or renewal transaction.

Sample request

The following is a sample pickup request:

```
GET https://pilot-certmanager-webservices.websecurity.symantec
.com/vswebservices/rest/services/pickup?transaction_id=7bad8d4596bd6
9cfe092b5decdba0aa1 HTTP/1.0
```

Sample response

The pickup transaction response returns a status code and message code that indicates success or failure. The following is a sample of a successful pickup transaction response:

```
HTTP/1.0 200 OK
Date: Wed, 28 Jan 2009 02:29:42 GMT
Server: Apache/2.0.63
Content-Type: application/xml;charset=UTF-8

<Response xmlns:tns="http://webservices.mpki4ssl.symantec.com"
xmlns="urn:symantec:api">
```

```
<StatusCode>0x00</StatusCode>
<Message>success</Message>
<Certificate>
-----BEGIN CERTIFICATE-----
MIIF2zCCBMOgAwIBAgIQWJYYBh2nI/b3aV2letdfBjANBgkqhkiG9w0BAQUFADCB
wzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZGb3IgVGVzdCBQdXJwb3NlcyBPbmx5MUMwQQYDVQQLEzpUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EvIChjKTA2MTUw
MwYDVQQDEyxWZXJpU2lnbiBDbGFzcyAzIEV4dGVuZGVkIFZhbGlkYXRpb24gVGVz
dCBDQTAeFw0wOTAxMjMwMDAwMDBaFw0xMDAxMzAyMzU5NTlaMIGjMRMwEQYLKwYB
BAGCNzwCAQMTAlVTMQswCQYDVQQGEwJVTTELMAkGA1UEERQCVFcxDzANBgNVBAgT
BlRhaXdhbjEPMA0GA1UEBxQGVGFpcGVpMR4wHAYDVQQJFBU0ODcgRS4gTWlkZGxl
ZmllbGQgUmQxDjAMBgNVBAoUBW1jZWxwMSAwHgYDVQQDFBd3c3Rlc3RzaXRlLnZl
cmlzaWduLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAp8FSWM61ULNs
jNa+omViYyZFP4B41P4tRSe/Np10kJ05k3TFH07N3rIhDjMNub/EVVRHJxflsJez
cEqqKsdfStJU+M5DA3rC9H6WmNLcMB2m4d+GUzhsQcNNoITHGhpz3eEO4KGjwy84
2R95CeZz0BmmYiiJG9QShHZVxdvSJ4kCAwEAAaOCAmswggJnMHYGA1UdEQRvMG2C
E3NhbjExMS52ZXJpc2lnbi5jb22CE3NhbjIyMi52ZXJpc2lnbi5jb22CE3NhbjMz
My52ZXJpc2lnbi5jb22CE3NhbjQ0NC52ZXJpc2lnbi5jb22CF3dzdGVzdHNpdGUu
dmVyaXNpZ24uY29tMAkGA1UdEwQCMAAwHQYDVR0OBBYEFJ4OA8IxkmM7OOg90/XK
xptBBOTVMAsGA1UdDwQEAwIFoDBCBgNVHR8EOzA5MDegNaAzhjFodHRwOi8vRVZT
ZWN1cmUtY3JsLnZlcmlzaWduLmNvbS9FVlNlY3VyZTIwMDYuY3JsMEQGA1UdIAQ9
MDswOQYLYIZIAYb4RQEHFwYwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVy
aXNpZ24uY29tL3JwYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHwYD
VR0jBBgwFoAUSPaFv6dlv/JSw1YL2SlZw6W4M3kwfAYIKwYBBQUHAQEEcDBuMC0G
CCsGAQUFBzABhiFodHRwOi8vRVZTZWN1cmUtb2NzcC52ZXJpc2lnbi5jb20wPQYI
KwYBBQUHMAKGMWh0dHA6Ly9FVlNlY3VyZS1haWEudmVyaXNpZ24uY29tL0VWU2Vj
dXJlMjAwNi5jZXIwbgYIKwYBBQUHAQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lm
MCEwHzAHBgUrDgMCGgQUS2u5KJYGDLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xv
Z28udmVyaXNpZ24uY29tL3ZzbG9nbzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQBx
ayS2ZSyTd96CJlPgDkyQpADi3V/DZ7oJIhISDrVF/afiGJlTkJii/S402uVyUonm
/uGtBvmuCNjVmpama4pOMgxDb+of6VBgDjhZnCZnDsw1bgetnMINwEdAyPoG0pym
pNxlokx2+JYlB9lzWyhhcvW7GJ2G6OpL7ZTPRta7aPf9C6Vn5vDfawVEe1v7JLTG
j5xFxGMFpQX1c3FdtExxmblrH2ssfU1lXPb9OsmelDSf+BQsy9LwJtoxFv2Q+Su4
lJkBhwwvRRGrXeBLTfFsMTeBwi1EpFgHbyQjQ+Omr5sYZrWNualUdbxvur6eijEX
Yueh0NtklbTeCpzXLc0I
-----END CERTIFICATE-----
</Certificate>
</Response>
```

Chapter 5

Renewing an SSL certificate

This chapter includes the following topics:

Overview of renewing an SSL certificate

This chapter includes detailed request and response information for certificate renewal transactions.

Request (renewal)

Renewing a certificate through VICE 2.0 is nearly identical to enrolling for a certificate. However, with a renewal transaction, the SSL certificate application also needs to provide one of the following to identify the certificate being renewed:

- The original certificate
- The original Transaction ID

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/renew

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/renew

Table 5-1 displays the renewal request parameters. Some parameters are required.

Note: The following table shows required parameters for a renewal request. You specify these in addition to the required enrollment parameters in Table 3-1.

Table 5-1 Renewal request parameters

Name	Data type	Required	Max Length	Description
original_certificate	Valid base-64 encoded certificate	■ Y, if original_transaction_id is not present ■ N, if original_transaction_id is present		The certificate that is being renewed
original_transaction_id	Text	■ Y, if original_certificate is not present ■ N, if original_certificate is present	32	The transaction ID of the certificate being renewed
original_challenge	Text	Y	32	The current challenge phrase for the certificate being renewed
challenge	Text	Y	32	The new challenge phrase for the requested certificate
serverType	Text	Y	64	See "Request (enrollment)" on page 16.
subject_alt_names	Text	N		Subject alternative names. See "Request (enrollment)" on page 16.
signatureAlgorithm	Text	N	32	Signature algorithm. See "Request (enrollment)" on page 16.
ctLogOption	Text	N		Certificate Transparency public or not. See "Request (enrollment)" on page 16.

Table 5-1 Renewal request parameters *(continued)*

Name	Data type	Required	Max Length	Description
specificEndDate	MM/DD/YYYY	N	10	The end date for the renewed certificate. The end date can be no more than 2 years from the validity start date for EV certificates, and no more than 3 years from the validity start date for other certificates. For this parameter to take effect, you must enable an option the Control Center. Go to the **Configuration** tab, **Enrollment** page, **Select Certificate Lifecycle Options** section, and select **Applicants can request a specific end date within the validity period**.

Sample request

The following is a sample of a successful renewal transaction request:

```
POST https://certmanager-webservices.websecurity.symantec
.com/vswebservices/rest/services/renew HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 905

original_transaction_id=6b671d141321a8d743ab5616051d4ec&original_
certificate=&firstName=John&middleInitial=&lastName=Doe&email=
johndoe@aaa.com&employeeID=1234&serverType=Netscape
```

Sample response

The renewal transaction response returns a status code and message code that indicates success or failure. The following is a sample response to a successful renewal transaction request:

```
HTTP/1.0 200 OK
Content-Type: text/xml
Server: Apache/2.0.63
Date: Mon, 27 Nov 2006 23:22:49 GMT
Content-Length: 1256
Connection: Close
```

```
<Response xmlns="urn:symantec:api">
 <StatusCode>0x00</StatusCode>
  <Message>success</Message>
  <transaction_id>98345f3ebc1ba8d743ab5616051d4ff3</transaction_id>
  <Certificate>
-----BEGIN CERTIFICATE-----
2aqMj1qYBueyV/lx7py5lvEE+4FL/vRRO1qT......
-----END CERTIFICATE-----
  </Certificate>
</Response>
```

Chapter 6

Revoking an SSL certificate

This chapter includes the following topics:

Overview of revoking an SSL certificate

This chapter includes detailed request and response information for revocation transactions.

Caution: Your application should be able to recognize the current status of the certificate before revoking it and should only revoke a valid certificate. Certificates with pending, expired, or other non-valid status should not be revoked. After the certificate is revoked, there is no way to undo the revocation.

Request (revocation)

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/revoke

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/revoke

Table 6-1 displays the revocation request's parameters.

Table 6-1 Revocation request parameters

Name	Data type	Required	Max Length	Description
certSerial	Text	Y	32	The certificate serial number. Must be 32 bytes.
reason	Text	Y	64	Use one of the following reasons: ■ Key compromise ■ CA compromise ■ Affiliation changed ■ Superseded ■ Cessation of operation ■ Certificate hold ■ Remove from CRL ■ Privilege withdrawn ■ AA compromise ■ Unspecified.
challenge	Text	Y	32	The original challenge phrase for the certificate.

Sample request

The following is a sample certificate revocation request:

```
 POST https://certmanager-webservices.websecurity.symantec.com
/vswebservices/rest/services/revoke HTTP/1.0
Content-Type: application/x-www-form-urlencoded
User-Agent: ACME Security Services
Host: certmanager-webservices.websecurity.symantec.com
Content-Length: 68

reportType=units&startDate=9%2F21%2F2013&endDate=10%2F21%2F2013
Content-Type: application/x-www-form-urlencoded
User-Agent: ACME Security Services
Host: certmanager-webservices.websecurity.symantec.com
Content-Length: 68
```

```
certSerial=98345f3ebc1ba8d743ab5616051d4ff3&challenge=
pass&reason=key+comprised&certProductType=Server
```

Sample response

The revocation response returns a status code and message code that indicates success or failure. The following is a sample of a successful revocation response:

```
HTTP/1.0 200 OK
Content-Type: text/xml
Server: Apache/2.1
Date: Mon, 8 Dec 2008 23:22:49 GMT
Content-Length: 112
Connection: Close

<Response xmlns="urn:symantec:api">
 <StatusCode>0x00</StatusCode>
  <Message>success</Message>
</Response>
```

Chapter 7

Replacing an SSL certificate

This chapter includes the following topics:

Overview of replacing an SSL certificate

Use this function to replace a valid certificate when the security of the certificate is compromised.

Request (replacement)

The request should contain the original certificate or transaction ID to retrieve the original transaction information for the certificate.

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/replace

Production endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/rest/services/replace

The following table shows required parameters for a replacement request.

Table 7-1 Replacement request parameters (required)

Name	Data type	Required	Max Length	Description
original_certificate	Valid base-64 encoded certificate	Required if original_transaction_id is not present		Base-64 encoded X.509 certificate from the original enrollment
original_transaction_id	Text	Required if original_certificate is not present.	32	Transaction id from the original enrollment
original_challenge	Text	Y	32	The challenge phrase from the original enrollment
challenge	Text	Y	32	A new challenge phrase for the requested certificate
reason	Text	Y	32	Reason for replacing the certificate. the section called “Request (revocation)”
specificEndDate	MM/DD/YYYY	N	10	The end date for the replacement certificate. The end date must precede the end of the validity period for this certificate. For this parameter to take effect, you must enable an option the Control Center. Go to the **Configuration** tab, **Enrollment** page, **Select Certificate Lifecycle Options** section, and select **Applicants can request a specific end date within the validity period**.

The following are optional. The system uses the information from the original certificate enrollment if they are not present. If you supply the following information, the new data overwrites the existing data.

Table 7-2 Replacement request parameters (optional)

Name	Data type	Required	Max Length	Description
firstName	Text	N	240	Subscriber's first name
middleInitial	Text	N	1	Subscriber's middle initial
lastName	Text	N	240	Subscriber's last name
email	Text	N		Subscriber's email address
csr	Base-64	N		Base-64 PKCS#10 formatted certificate signing request.
serverType	Text	Y	64	See "Request (enrollment)" on page 16.
comment/addtional_field3	T61	N	512	Comments from the subscriber.
jobTitle	T61	N	64	Job title. This is configured as either required or optional in the Control Center, but is overwritten by the API value.
employeeID	T61	N	64	Employee ID. This is configured as either required or optional in the Control Center, but is overwritten by the API value.
serverIP /additional_field10	T61	N	64	Server IP. This is configured as either required or optional in the Control Center, but is overwritten by the API value.
mailStop	T61	N	64	Mail Stop. This is configured as either required or optional in the Control Center, but is overwritten by the API value.
additional_field#0	T61	N	64	Additional field #. See "Request (enrollment)" on page 16.
subject_alt_name#	Text	N	50	Subject alternative name. See "Request (enrollment)" on page 16.
subject_alt_names	Text	N		Subject alternative names. See "Request (enrollment)" on page 16.
signatureAlgorithm	Text	N	32	Signature algorithm. See "Request (enrollment)" on page 16.

Table 7-2 Replacement request parameters (optional) *(continued)*

Name	Data type	Required	Max Length	Description
ctLogOption	Text	N		Certificate Transparency public or not. See "Request (enrollment)" on page 16.

Sample request

The following is a sample of a successful renewal request:

```
POST
https://certmanager-webservices.websecurity.symantec.com
/vswebservices/rest/services/renew HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 905

original_transaction_id=6b671d141321a8d743ab5616051d4ec&original_certifi
cate=&firstName=John&middleInitial=&lastName=Doe&email=johndoe@aaa.com&e
mployeeID=1234&serverType=Netscape
```

Sample response

The renewal response returns a status code and message code that indicates success or failure. The following is a sample response to a successful renewal request:

```
HTTP/1.0 200 OK
Content-Type: text/xml
Server: Apache/2.0.63
Date: Mon, 27 Nov 2006 23:22:49 GMT
Content-Length: 1256
Connection: Close

<Response xmlns="urn:symantec:api">
 <StatusCode>0x00</StatusCode>
  <Message>success</Message>
  <transaction_id>98345f3ebc1ba8d743ab5616051d4ff3</transaction_id>
  <Certificate>
-----BEGIN CERTIFICATE-----
2aqMj1qYBueyV/lx7py5lvEE+4FL/vRRO1qT......
-----END CERTIFICATE-----
```

```
  </Certificate>
</Response>
```

Chapter 8

Approving an order

This chapter includes the following topics:

Overview of approving an order

Approve an order by passing the transaction ID into the approval request.

Request (approval)

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/approve

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/approve

Table 8-1 Approval request parameters

Name	Data type	Required	Max Length	Description
transaction_id	Text	Required if orderNumber is not present.	32	The enrollment order's transaction ID.

Sample request

Use the GET or POST method with your approval request.

```
POST /vswebservices/rest/services/approve HTTP/1.0
Content-Type: application/x-www-form-urlencoded
User-Agent: ACME Security Services
Host: certmanager-webservices.websecurity.symantec
Content-Length: 57

transaction_id=98345f3ebc1ba8d743ab5616051d4ff3
```

```
GET /vswebservices/rest/services/approve?transaction_id=98345f3ebc1ba8
d743ab5616051d4ff3 HTTP/1.0
```

Sample response

```
HTTP/1.0 200 OK
Content-Type: text/xml
Date: Mon, 12 Jan 2015 23:22:49 GMT
Content-Length: 1356
Connection: Close

<Response xmlns="urn:verisign:api" xmlns:tns="http://webservices
.mpki4ssl.verisign.com">
  <StatusCode>0x00</StatusCode>
  <Message>certificate approved</Message>
  <Certificate>
-----BEGIN CERTIFICATE-----
MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCBJYwggP/oAMC
AQICEAHylxIQ0fJuHI7ThGImWccwDQYJKoZIhvcNAQEFBQAwgboxHzAdBgNVBAoT
FlZlcmlTaWduIFRydXN0IE5ldHdvcmsxFzAVBgNVBAsTDlZlcmlTaWduLCBJbmMu
. . .
AQQFAANBAPD3kw9bU1xRbZK+7K7SbBWNMq26iRbx9+wTAK2jpBH9WywDgC0nOrAY
R5BieNf+4BNXKEwPqUJnhymMssZuuvUAADEAAAAAAAAA
-----END CERTIFICATE-----
  </Certificate>
  <CertificateFormat>x509</CertificateFormat>
  </Response>
```

Chapter 9

Rejecting an order

This chapter includes the following topics:

Overview of rejecting an order

Reject an order by passing the transaction ID into the reject request.

Request (reject)

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/reject

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/reject

Table 9-1 Reject request parameters

Name	Data type	Required	Max Length	Description
transaction_id	Text	Required if orderNumber is not present.	32	The enrollment order's transaction ID.

Sample request

Use the GET method with the reject request.

```
GET /vswebservices/rest/services/reject?transaction_id=7bad8d4596bd6
9cfe092b5decdba0aa1 HTTP/1.0
```

Sample response

```
HTTP/1.0 200 OK
Content-Type: text/xml
Date: Mon, 12 Jan 2015 23:22:49 GMT
Content-Length: 193
Connection: Close

<Response xmlns="urn:verisign:api"
  xmlns:tns="http://webservices.mpki4ssl.verisign.com">
  <StatusCode>0x00</StatusCode>
  <Message>certificate successfully rejected</Message>
  </Response>
```

Chapter 10

Getting an alternate SSL certificate

This chapter includes the following topics:

Overview of getting an alternate SSL certificate

Use this service to get an alternate version of an existing valid certificate. The alternate certificate has a different public key type. For premium certificates (Premium SSL, Premium Intranet SSL, and Premium Extended Validation SSL), you can get RSA, DSA, and ECC certificates for the same distinguished name (DN). For Standard SSL, Standard Intranet SSL, OFX SSL, and Standard Extended Validation SSL, you can get RSA and DSA versions for the same DN.

Request (get alternate)

Request should contain the original certificate or transaction ID to retrieve the original transaction information for the certificate.

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/getAlternate

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/getAlternate

The following table shows required parameters for a get alternate certificate request.

Table 10-1 Get alternate certificate request parameters (required)

Name	Data type	Required	Max Length	Description
original_certificate	Text (Base64 encoded)	Required if original_transaction_id is not present.		Base-64 encoded X.509 certificate from the original enrollment
original_transaction_id	Text	Required if original_certificate is not present.	32	Transaction ID from the original enrollment
original_challenge	Text	Y	32	The challenge phrase from the original enrollment
challenge	Text	Y	32	A new challenge phrase for the requested certificate
csr	Text (Base64 encoded)	N		A base-64 encoded PKCS#10 CSR.

The following are optional. The system uses the information from the original certificate enrollment if they are not present. If you supply the following information, the new data overwrites the existing data.

Table 10-2 Get alternate certificate parameters (optional)

Name	Data type	Required	Max Length	Description
firstName	Text	N	240	Subscriber's first name
middleInitial	Text	N	1	Subscriber's middle initial
lastName	Text	N	240	Subscriber's last name
email	Text	N		Subscriber's email address
certProductType	Text	N	32	See "Request (enrollment)" on page 16.
serverType	Text	N	64	See "Request (enrollment)" on page 16.

Table 10-2 Get alternate certificate parameters (optional) *(continued)*

Name	Data type	Required	Max Length	Description
employeeID	T61	N	64	Employee ID. This is configured as either required or optional in the Control Center, but is overwritten by the API value.
serverIP /additional_field10	T61	N	64	Server IP. This is configured as either required or optional in the Control Center, but is overwritten by the API value.
mailStop	T61	N	64	Mail Stop. This is configured as either required or optional in the Control Center, but is overwritten by the API value.
additional_field#0	T61	N	64	Additional field #. See "Request (enrollment)" on page 16.
signatureAlgorithm	Text	N	32	Signature algorithm. See "Request (enrollment)" on page 16.
ctLogOption	Text	N		Certificate Transparency public or not. See "Request (enrollment)" on page 16.

Sample request

The following is a sample of a successful renewal request:

```
POST
https://certmanager-webservices.websecurity.symantec.com
/vswebservices/rest/services/renew HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 905

original_transaction_id=6b671d141321a8d743ab5616051d4ec&original_
certificate=&firstName=John&middleInitial=&lastName=Doe&email=
johndoe@aaa.com&employeeID=1234&serverType=Netscape
```

Sample response

The renewal response returns a status code and message code that indicates success or failure. The following is a sample response to a successful renewal request:

```
HTTP/1.0 200 OK
Content-Type: text/xml
Server: Apache/2.0.63
Date: Mon, 27 Nov 2006 23:22:49 GMT
Content-Length: 1256
Connection: Close

<Response xmlns="urn:symantec:api">
 <StatusCode>0x00</StatusCode>
  <Message>success</Message>
  <transaction_id>98345f3ebc1ba8d743ab5616051d4ff3</transaction_id>
  <Certificate>
-----BEGIN CERTIFICATE-----
2aqMj1qYBueyV/lx7py5lvEE+4FL/vRRO1qT......
-----END CERTIFICATE-----
  </Certificate>
</Response>
```

Chapter 11

Retrieving total available SSL certificate units

This chapter includes the following topics:

Overview of retrieving total available SSL certificate units

This chapter describes request and response information for certificate unit summary transactions. This transaction checks how many SSL certificate units remain in your account and returns counts of ordered, used, and remaining units.

If you only want information about SSL certificate units within a specified time frame, use the units report request. See “Request units report” on page 71.

Request

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/gettokencounts

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/gettokencounts

This request does not require parameters.

Sample request

The following is a sample certificate unit availability request:

```
GET https://certmanager-webservices.websecurity.symantec.com
/vswebservices/rest/services/gettokencounts HTTP/1.0
```

Sample response

The response returns a status code and message code that indicates success or failure. The following is a sample of a successful retrieval response:

```
HTTP/1.0 200 OK
Content-Type: text/xml
Server: Apache/2.0.63
Date: Mon, 8 Dec 2008 23:22:49 GMT
Content-Length: 475
Connection: Close
<Response xmlns="urn:symantec:api">
<StatusCode>0x00</StatusCode>
<Message>success</Message>
<tokenCount type="Server" ordered="100" used="5" remaining="95"/>
<tokenCount type="GlobalServer" ordered="100" used="20" remaining="80"/>
<tokenCount type="IntranetServer" ordered="0" used="0" remaining="0"/>
<tokenCount type="IntranetGlobalServer" ordered="0" used="0"
remaining="0"/>
<tokenCount type="OFXServer" ordered="0" used="0" remaining="0"/>
</Response>
```

Chapter 12

Retrieving certificate unit details

This chapter includes the following topics:

Overview of retrieving certificate unit details

This chapter describes request and response information to retrieve details for the certificate units in your account. It provides details of each unit order, including order number, units purchased, used, and remaining, and the expiration date of the units. This is the same data that you can view in the Certificate Management landing page in the Control Center.

Request

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/getTokens

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/getTokens

There are no parameters for this request. Your jurisdiction is identified by your administrator ID.

The following is a sample request for details of the SSL certificate units in your account using the POST method:

```
POST https://certmanager-webservices.websecurity.symantec
.com/vswebservices/rest/services/getTokens HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 1301
```

Sample response

After the request is submitted, the service sends an HTTP response to the requesting application. The following is a sample of a successful response:

```
<Response xmlns:tns="http://webservices.mpki4ssl.symantec.com">
 <StatusCode>0x00</StatusCode>
 <Message>success</Message>
 <Order type="AdminID" orderNumber="126569530" ordered="6" used="0"
  remaining="6" expiration="JUN 16, 2012" />
 <Order type="AdminID" orderNumber="126569486" ordered="5" used="5"
  remaining="0" expiration="JUN 16, 2012" />
 <Order type="DomainName" orderNumber="126853450" ordered="100" used="0"
  remaining="100" expiration="AUG 18, 2012" />
 <Order type="HAServer" orderNumber="127001755" ordered="1000" used="27"
  remaining="973" expiration="SEP 22, 2012" />
 <Order type="Server" orderNumber="126569448" ordered="11" used="0"
  remaining="11" expiration="JUN 16, 2012" />
 <Order type="GlobalServer" orderNumber="126747113" ordered="10" used="0"
  remaining="10" expiration="JUL 27, 2012" />
 <Order type="IntranetServer" orderNumber="126102627" ordered="2000"
  used="511" remaining="1489" expiration="MAR 29, 2012" />
 <Order type="IntranetGlobalServer" orderNumber="126894195" ordered="1000"
  used="41" remaining="959" expiration="AUG 24, 2012" />
 <Order type="OFXServer" orderNumber="126901405" ordered="500" used="64"
  remaining="436" expiration="AUG 25, 2012" />


</Response>
```

Chapter 13

Retrieving customized enrollment fields

This chapter includes the following topics:

Overview of retrieving customized enrollment fields

This chapter describes request and response information to retrieve custom fields that administrators configured for a certificate enrollment form. Administrators use the Enrollment Wizard in the Control Center to create the custom fields.

Request

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/getEnrollmentFields

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/getEnrollmentFields

There are no parameters for this request. Your jurisdiction is identified by your administrator ID.

The following is a sample request to retrieve custom fields using the POST method:

```
POST https://certmanager-webservices.websecurity.symantec
.com/vswebservices/rest/services/getEnrollmentFields HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 1301
```

Sample response

After the request is submitted, the service sends an HTTP response to the requesting application. The following is a sample of a successful enrollment response:

```
HTTP/1.0 200 OK
Date: Tue, 27 Apr 2012 18:07:07 GMT
Server: Apache/2.0.63
Connection: Close
Content-Type: application/xml;charset=UTF-8
Content-Length: 2815

<Response xmlns:tns="http://webservices.mpki4ssl.symantec.com">
<StatusCode>0x00</StatusCode>
<Message>success</Message>
<Field name="firstName" label="First Name" include="Yes" required="Yes" />
<Field name="lastName" label="Last Name" include="Yes" required="Yes" />
<Field name="email" label="Email Address" include="Yes" required="Yes" />
<Field name="jobTitle" label="Title" include="No" required="No" />
<Field name="employeeID" label="Employee ID Number" include="No"
required="No" />
<Field name="mailStop" label="Mail Stop" include="No" required="No" />
<Field name="departmentNo" label="Department No" include="No" required="No"
 />
<Field name="serverIP" label="Server IP" include="No" required="No" />
- <Field name="additionalFieldField_1" label="Mobile Phone No."
include="Yes" required="No">
  <Description />
  <DropdownOptions />
  </Field>
- <Field name="additionalField2" label="" include="No" required="No">
  <Description />
  <DropdownOptions />
  </Field>
- <Field name="additionalField3" label="" include="No" required="No">
  <Description />
```

```
  <DropdownOptions />
  </Field>
- <Field name="additionalField4" label="" include="No" required="No">
  <Description />
  <DropdownOptions />
  </Field>
- <Field name="additionalField5" label="" include="No" required="No">
  <Description />
  <DropdownOptions />
  </Field>
- <Field name="additionalField6" label="" include="No" required="No">
  <Description />
  <DropdownOptions />
  </Field>
- <Field name="additionalField7" label="" include="No" required="No">
  <Description />
  <DropdownOptions />
  </Field>
- <Field name="additionalField8" label="" include="No" required="No">
  <Description />
  <DropdownOptions />
  </Field>
- <Field name="additionalField9" label="" include="No" required="No">
  <Description />
  <DropdownOptions />
  </Field>
- <Field name="additionalField10" label="" include="No" required="No">
  <Description />
  <DropdownOptions />
  </Field>
  </Response>
```

Chapter 14

Retrieving vetted organizations and domains

This chapter includes the following topics:

Overview of retrieving vetted organizations and domains

This chapter describes request and response information to retrieve the organizations and domains that Symantec has authenticated for your account.

Request

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/getVettedOrgsAndDomains

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/rest/services/getVettedOrgsAndDomains

There are no parameters for this request. Your jurisdiction is identified by your administrator ID.

The following is a sample request for organizations and domains using the POST method:

```
POST https://certmanager-webservices.websecurity.symantec
.com/vswebservices/rest/services/getVettedOrgsAndDomains HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 1301
```

Sample response

After the request is submitted, the service sends an HTTP response to the requesting application. The following is a sample of a successful response:

```
HTTP/1.0 200 OK
Date: Tue, 27 Apr 2012 18:07:07 GMT
Server: Apache/2.0.63
Connection: Close
Content-Type: application/xml;charset=UTF-8
Content-Length: 2815

<Response xmlns:tns="http://webservices.mpki4ssl.symantec.com">
  <StatusCode>0x00</StatusCode>
  <Message>success</Message>
 <Organization name="ABCD Inc" EV_Enabled="No">
  <Domain EV_Enabled="No">103.com</Domain>
  <Domain EV_Enabled="No">104.com</Domain>
  <Domain EV_Enabled="No">add5.com</Domain>
  </Organization>
  <Organization name="EFGH Inc." EV_Enabled="Yes">
  <Domain EV_Enabled="Yes">add2.dom</Domain>
  <Domain EV_Enabled="No">add5.com</Domain>
  <Domain EV_Enabled="Yes">dfsdf-cdf.dff-df.com</Domain>
  <Domain EV_Enabled="Yes">dsdd.c-m</Domain>
  </Organization>
</Response>
```

Chapter 15

Running a report

This chapter includes the following topics:

Overview of running a report

This chapter describes request and response information for real-time reports. You can use the API to run three report types:

- Detail report: Corresponds to the Detail real-time report in the Control Center.
- Summary report: Corresponds to the Summary real-time report in the Control Center.
- Units report: Corresponds to the Units real-time report in the Control Center. This report returns similar information to the getTokenCounts request within a specified time frame.

Request detail report

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/reportingws

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/reportingws

Table 15-3 lists the parameters for the report request. Some parameters are required.

Table 15-1 Detail report request parameters

Name	Data type	Required	Max Length	Description
reportType	Text	Y	32	For a Detail report, the value is `detail`.
startDate	Date	Y	10	Start date of the report, in MM/DD/YYYY format. The start date and date range can be six years apart, maximum.
endDate	Date	Y	10	End date of the report, in MM/DD/YYYY format. The start date and date range can be six years apart, maximum.
certProductType	Text	N		Takes one of the following values: ■ `All`. This is the default value. ■ `HAServer` ■ `HAGlobalServer` ■ `Server` ■ `GlobalServer` ■ `IntranetServer` ■ `IntranetGlobalServer` ■ `PrivateServer` ■ `OFXServer` ■ `GeotrustServer`
organization	Text	N	64	The name of a vetted organization. The default is a report of all organizations.
organizationalUnit	Text	N	64	The name of an organizational unit within the organization.

Table 15-1 Detail report request parameters *(continued)*

Name	Data type	Required	Max Length	Description
certStatus	Text	N	64	Takes one of the following values: ■ `All`. This is the default value. It is also used if you omit this parameter or leave its value empty. ■ `Pending` ■ `Approved` ■ `Rejected` ■ `Valid` ■ `Revoked` ■ `Deactivated` ■ `Expired`
customizedColumnsOnly	Text	N	1	The value can be `Y` or `N`. If the value is `Y`, the API only returns data from the selected custom columns in the Control Center. You can retrieve the custom columns using the `getCustomizedColumns` call. See "Overview of retrieving custom report fields" on page 74.
structuredRecord	Text	N	1	The value can be `Y` or `N`. If the value is `Y`, each row of the response contains the information for a particular certificate. If the value is `no`, the response is organized according to each column in the report.

Sample detail report request

The following is a sample detail report request using the POST method:

```
POST https://certmanager-webservices.websecurity.symantec
.com/vswebservices/reportingws
Content-Type: application/x-www-form-urlencoded
User-Agent: ACME Security Services
Host: certmanager-webservices.websecurity.symantec.com
Content-Length: 68

reportType=detail&startDate=9%2F21%2F2013&endDate=10%2F21%2F2013
&organization=&orgUnit=&certProductType=GlobalServer&certStatus=
Valid&customizedColumnsOnly=Y&structuredRecord=N
```

Sample detail report response

After the request is submitted, the service sends an HTTP response to the requesting application.

The following is a sample of a successful detail report transaction response. Each component in the response is organized by report column (`structuredRecord=N`). You can also request a report organized by certificate (`structuredRecord=Y`).


```
{
  "certificateType": [
    "Code Signing for Authenticode",
    "Standard SSL",
    "Code Signing for Authenticode",
    "Code Signing for Java",
    "Standard EV SSL",
  ],
  "status": [
    "Valid",
    "Valid",
    "Valid",
    "Pending",
    "Valid",
  ],
  "commonName": [
    "example.com",
    "1234.company.com",
    "example",
    "5678.example.com",
    "company.com",
   ],
  "organizationalUnit": [
    "myorgunit1",
    "myorgunit2",
    "exampleorgunit1",
    "exampleorgunit2",
    "myorgunit3",
    ],
  "organization": [
    "company",
    "company",
    "company",
    "company",
    "company",
```

```
  ],
"locality": [
  "Mountain View",
  "Mountain View",
  "Mountain View",
  "Mountain View",
  "Mountain View",
  ],
"state": [
  "California",
  "California",
  "California",
  "California",
  "California",
   ],
"country": [
  "US",
  "US",
  "US",
  "US",
  "US",
  ],
"subjectAlternativeNames": [
  "1.company.com",
  "2.company.com",
  "3.company.com",
  "4.company.com",
  "5.company.com",
   ],
"certificateSerialNumber": [
  "2f9db7fbdd83185642d84082df1f5a5e",
  "32db0f9797fbb3a88c0181e9580b70ac",
  "374aeb7ba66a5cd73ab46b3de117938a",
  "12b1cdb014d7c8a0d9b7c0b8b61a7b76",
  "0376c690974b51876f3b749936a73363",
  ],
"validityStartDate": [
  "11-SEP-2013",
  "10-SEP-2013",
  "10-SEP-2013",
  "17-SEP-2013",
  "03-OCT-2013",
   ],
```

```
"validityEndDate": [
  "23-JUL-2015",
  "11-SEP-2015",
  "11-SEP-2015",
  "17-SEP-2015",
  "03-OCT-2015",
   ],
"revocationDate": [
  "N/A",
  "N/A",
  "N/A",
  "N/A",
  "16-SEP-2013"
 ],
"licenses": [
  1,
  1,
  1,
  1,
  1,
],
"totalUnits": [
  1,
  1,
  1,
  0,
  4,
],
"requestType": [
  "replacement",
  "enrollment",
  "enrollment",
  "enrollment",
  "renewal",
 ],
"serverType": [
  "Server Type - Netscape",
  "",

  "Server Type - Netscape",
  "Server Type - iPlanet",
],
"email": [
```

```
  "employee1@company.com",
  "employee2@company.com",
  "employee3@company.com",
  "employee4@company.com",
  "employee5@company.com",
],
"title": [
  "security admin",
  "admin",
  "admin",
  "admin",
  "",
 ],
"employeeID": [
  "1234",
  "5678",
  "9101",
  "1213",
  "1415",
 ],
"mailStop": [
  "",
  "",
  "",
  "",
  "",
   ],
"departmentNumber": [
  "",
  "",
  "",
  "",
  "",
 ],
"serverIP": [
  "",
  "",
  "",
  "",
  "",
],
"userComment": [
  "",
```

```
      "",
      "",
      "",
      "",
    ],
    "assignedTo": [
      "",
      "",
      "",
      "",
      "",
    ],
    "firstName": [
      "John",
      "Jane",
      "John",
      "Jane",
      "John",
    ],
    "lastName": [
      "Doe",
      "Doe",
      "Doe",
      "Doe",
      "Doe",
    ],
    "keyInfo": [
      "RSA 2048-bit",
      "RSA 2048-bit",
      "RSA 2048-bit",
      "RSA 2048-bit",
      "RSA 2048-bit",
  ],
    "paymentTerm": [
      "1-Year",
      "1-Year",
      "2-Year",
      "2-Year",
      "2-Year",
    ],
    "expressRenewal": [
      "Deactivated",
      "Deactivated",
```

```
      "Deactivated",
      "Deactivated",
      "Deactivated",
    ],
    "autoRedeem": [
      "Deactivated",
      "Deactivated",
      "Deactivated",
      "Deactivated",
      "Deactivated",
    ],
    "termRenewalDate": [
      "18-JUL-2013",
      "22-SEP-2013",
      "22-SEP-2013",
      "22-SEP-2013",
      "22-SEP-2013",
    ],
    "signatureAlgorithm": [
      "SHA-1 with RSA Encryption",
      "SHA-1 with RSA Encryption",
      "SHA-1 with RSA Encryption",
      "SHA-1 with RSA Encryption",
      "SHA-1 with RSA Encryption",
    ],
    "numberOfFQDNs": [
      10,
      0,
      0,
      0,
      0,
    ]
}
```


Request summary report

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/reportingws

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/reportingws

Table 15-3 lists the parameters for the report request. Some parameters are required.

Table 15-2 Summary report request parameters

Name	Data type	Required	Max Length	Description
reportType	Text	Y	32	For a Summary report, the value is `summary`.
startDate	Date	Y	10	Start date of the report, in MM/DD/YYYY format. The start date and date range can be six years apart, maximum.
endDate	Date	Y	10	End date of the report, in MM/DD/YYYY format. The start date and date range can be six years apart, maximum.
certProductType	Text	N		Takes one of the following values: ■ `All`. This is the default value. ■ `HAServer` ■ `HAGlobalServer` ■ `Server` ■ `GlobalServer` ■ `IntranetServer` ■ `IntranetGlobalServer` ■ `PrivateServer` ■ `OFXServer` ■ `GeotrustServer`
organization	Text	N	64	The name of a vetted organization. The default is a report of all organizations.
organizationalUnit	Text	N	64	The name of an organizational unit within the organization.

Sample summary report request

The following is a sample report request using the POST method:

```
POST https://certmanager-webservices.websecurity.symantec.com/vswebservices/r
Content-Type: application/x-www-form-urlencoded
User-Agent: ACME Security Services
```

```
Host: certmanager-webservices.websecurity.symantec.com
Content-Length: 68

reportType=summary&startDate=9%2F21%2F2013&endDate=9%2F21%2F2013
&organization=&orgUnit=&certProductType=Server
```

Sample summary report response

After the request is submitted, the service sends an HTTP response to the requesting application.

The following is a sample of a successful summary report response:

```
{
  "certificateSummary": [
    {
      "productType": "Standard SSL",
      "Pending": 0,
      "Approved": 0,
      "Rejected": 0,
      "Valid": 4,
      "Revoked": 11,
      "Expired": 8,
      "Deactivated": 0
    },
    {
      "productType": "Premium SSL",
      "Pending": 0,
      "Approved": 0,
      "Rejected": 0,
      "Valid": 0,
      "Revoked": 6,
      "Expired": 7,
      "Deactivated": 0
    },
    {
      "productType": "Standard EV SSL",
      "Pending": 0,
      "Approved": 0,
      "Rejected": 0,
      "Valid": 2,
      "Revoked": 0,
      "Expired": 11,
      "Deactivated": 0
```

```
},
{
  "productType": "Premium EV SSL",
  "Pending": 0,
  "Approved": 0,
  "Rejected": 0,
  "Valid": 0,
  "Revoked": 0,
  "Expired": 8,
  "Deactivated": 0
},
{
  "productType": "Standard Intranet SSL",
  "Pending": 0,
  "Approved": 0,
  "Rejected": 0,
  "Valid": 0,
  "Revoked": 4,
  "Expired": 1,
  "Deactivated": 0
},
{
  "productType": "Premium Intranet SSL",
  "Pending": 0,
  "Approved": 0,
  "Rejected": 0,
  "Valid": 0,
  "Revoked": 5,
  "Expired": 2,
  "Deactivated": 0
},
{
  "productType": "Wildcard SSL",
  "Pending": 0,
  "Approved": 0,
  "Rejected": 0,
  "Valid": 0,
  "Revoked": 0,
  "Expired": 1,
  "Deactivated": 0
},
{
  "productType": "RapidSSL Enterprise",
```

```
  "Pending": 0,
  "Approved": 0,
  "Rejected": 0,
  "Valid": 0,
  "Revoked": 3,
  "Expired": 5,
  "Deactivated": 0
},
{
  "productType": "OFX SSL",
  "Pending": 0,
  "Approved": 0,
  "Rejected": 0,
  "Valid": 1,
  "Revoked": 0,
  "Expired": 1,
  "Deactivated": 0
},
{
  "productType": "Code Signing for Authenticode",
  "Pending": 0,
  "Approved": 0,
  "Rejected": 0,
  "Valid": 2,
  "Revoked": 0,
  "Expired": 5,
  "Deactivated": 0
},
{
  "productType": "Code Signing for Java",
  "Pending": 1,
  "Approved": 0,
  "Rejected": 0,
  "Valid": 0,
  "Revoked": 0,
  "Expired": 0,
  "Deactivated": 0
},
{
  "productType": "ECC SSL",
  "Pending": 0,
  "Approved": 0,
  "Rejected": 0,
```

```
      "Valid": 0,
      "Revoked": 0,
      "Expired": 0,
      "Deactivated": 0
    }
  ]
}
```

Request units report

The request for a units report is similar to the getTokenCounts request, but it returns information within a specified time frame. See "Overview of retrieving total available SSL certificate units" on page 49.

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/reportingws

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/reportingws

Table 15-3 lists the parameters for the report request. Some parameters are required.

Table 15-3 Report request parameters

Name	Data type	Required	Max Length	Description
reportType	Text	Y	32	For a Units report, the value is `units`.
startDate	Date	Y	10	Start date of the report, in MM/DD/YYYY format. The start date and date range can be six years apart, maximum.
endDate	Date	Y	10	End date of the report, in MM/DD/YYYY format. The start date and date range can be six years apart, maximum.

Sample units report request

The following is a sample report request using the POST method:

```
POST https://certmanager-webservices.websecurity.symantec
.com/vswebservices/reportingws
Content-Type: application/x-www-form-urlencoded
```

```
User-Agent: ACME Security Services
Host: certmanager-webservices.websecurity.symantec.com
Content-Length: 68

reportType=units&startDate=9%2F21%2F2013&endDate=10%2F21%2F2013
```

Sample units report response

After the request is submitted, the service sends an HTTP response to the requesting application.

The following is a sample of a successful units report response:

```
{
  "unitOrders": [
    {
      "productType": "Administrator IDs",
      "orderType": [
        "Customer Service",
        "Promotion"
      ],
      "orderNumber": [
        "133595373",
        "133598544"
      ],
      "ordered": [
        500,
        3
      ],
      "used": [
        1,
        0
      ],
      "remaining": [
        499,
        3
      ],
      "expiration": [
        "03-OCT-2014",
        "13-MAR-2014"
      ]
    },
    {
      "productType": "Domain Names",
```

```
      "orderType": [
        "Promotion"
      ],
      "orderNumber": [
        "133598544"
      ],
      "ordered": [
        10
      ],
      "used": [
        0
      ],
      "remaining": [
        10
      ],
      "expiration": [
        "13-MAR-2014"
      ]
    }
  ]
}
```

Chapter 16

Retrieving custom report fields

This chapter includes the following topics:

Overview of retrieving custom report fields

This chapter describes request and response information to retrieve the custom fields that you have defined for a detailed real-time reports in the Control Center.

Request

Service endpoints

Pilot endpoint:

https://pilot-certmanager-webservices.websecurity.symantec.com/vswebservices/getConfig?op=getCustomizedColumns

Production endpoint:

https://certmanager-webservices.websecurity.symantec.com/vswebservices/getConfig?op=getCustomizedColumns

There are no parameters for this request. Your administrator ID identifies your jurisdiction.

The following is a sample request for customized columns. This request always uses the GET method:

```
GET https://pilot-certmanager-webservices.websecurity.symantec.com
/vswebservices/getConfig?op=getCustomizedColumns
```

Sample response

After the request is submitted, the service sends an HTTP response to the requesting application. The following is a sample of a successful response:


```
{
  "selectedColumns": [
    {
      "variableName": "keyInfo",
      "displayName": "Key Info"
    },
    {
      "variableName": "commonName",
      "displayName": "Common Name"
    },
    {
      "variableName": "organizationalUnit",
      "displayName": "Organizational Unit"
    },
    {
      "variableName": "organization",
      "displayName": "Organization"
    },
    {
      "variableName": "locality",
      "displayName": "Locality"
    },
    {
      "variableName": "state",
      "displayName": "State"
    },
    {
      "variableName": "country",
      "displayName": "Country"
    },
    {
      "variableName": "certificateSerialNumber",
```

```
  "displayName": "Certificate Serial Number"
},
{
  "variableName": "validityStartDate",
  "displayName": "Validity Start Date"
},
{
  "variableName": "validityEndDate",
  "displayName": "Validity End Date"
},
{
  "variableName": "revocationDate",
  "displayName": "Revocation/Deactivation Date"
},
{
  "variableName": "licenses",
  "displayName": "Licenses"
},
{
  "variableName": "totalUnits",
  "displayName": "Total Units"
},
{
  "variableName": "requestType",
  "displayName": "Request Type"
},
{
  "variableName": "serverType",
  "displayName": "Server Type"
},
{
  "variableName": "email",
  "displayName": "Email"
},
{
  "variableName": "subjectAlternativeNames",
  "displayName": "Subject Alternative Names"
},
{
  "variableName": "firstName",
  "displayName": "First Name"
},
{
```

```
  "variableName": "lastName",
  "displayName": "Last Name"
},
{
  "variableName": "title",
  "displayName": "Title"
},
{
  "variableName": "employeeId",
  "displayName": "Employee Id"
},
{
  "variableName": "mailStop",
  "displayName": "Mail Stop"
},
{
  "variableName": "departmentNumber",
  "displayName": "Department No."
},
{
  "variableName": "serverIP",
  "displayName": "Server IP"
},
{
  "variableName": "additionalField",
  "displayName": "addl 1"
},
{
  "variableName": "additionalField",
  "displayName": "addl 2"
},
{
  "variableName": "userComment",
  "displayName": "User Comment"
},
{
  "variableName": "assignedTo",
  "displayName": "Assigned To"
},
{
  "variableName": "certificateType",
  "displayName": "Certificate Type"
},
```

```
{
  "variableName": "paymentTerm",
  "displayName": "Payment Term"
},
{
  "variableName": "expressRenewal",
  "displayName": "Express Renewal"
},
{
  "variableName": "autoRedeem",
  "displayName": "AutoRedeem"
},
{
  "variableName": "termRenewalDate",
  "displayName": "Term Renewal Date"
},
{
  "variableName": "additionalField",
  "displayName": "addl 3"
},
{
  "variableName": "additionalField",
  "displayName": "addl a"
},
{
  "variableName": "additionalField",
  "displayName": "addl 4"
},
{
  "variableName": "additionalField",
  "displayName": "addl 5"
},
{
  "variableName": "additionalField",
  "displayName": "addl 6"
},
{
  "variableName": "additionalField",
  "displayName": "addl 8"
},
{
  "variableName": "additionalField",
  "displayName": "addl 9"
```

```
    },
    {
      "variableName": "signatureAlgorithm",
      "displayName": "Signature Algorithm"
    },
    {
      "variableName": "additionalField",
      "displayName": "addl 7"
    },
    {
      "variableName": "numberOfFQDNs",
      "displayName": "Number Of FQDNs"
    }
  ]
}
```