

Cipher Suites and Their Names in the SCA

Contents

[Introduction](#)

[Before You Begin](#)

[Conventions](#)

[Prerequisites](#)

[Components Used](#)

[Matrix](#)

[SSL Version 2.0 Suites](#)

[SSL Version 3.0 Suites](#)

[TLS Version 1.0 Suites](#)

[Additional Export 1024 and Other Cipher Suites](#)

[Related Information](#)

Introduction

This document matches the full names of the various Secure Socket Layer/Transport Layer Security (SSL/TLS) cipher suites with the names that are used in the Secure Content Accelerator (SCA) for each cipher suite.

Before You Begin

Conventions

For more information on document conventions, see the [Cisco Technical Tips Conventions](#).

Prerequisites

Readers of this document should be knowledgeable of the following:

- SSL and cipher suites
- SCA configuration

Components Used

The information in this document is based on all versions of the CSS SCA.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Matrix

SSL Version 2.0 Suites

SSL/TLS Cipher Suites	SCA Cipher Suites
SSL_CK_RC4_128_WITH_MD5	ARC4-MD5
SSL_CK_RC4_128_EXPORT40_WITH_MD5	EXP-ARC4-MD5
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	EXP-ARC2-MD5
SSL_CK_DES_64_CBC_WITH_MD5	DES-CBC-MD5

SSL_CK_DES_192_EDE3_CBC_WITH_MD5	DES- CBC3- MD5
----------------------------------	----------------------

SSL Version 3.0 Suites

SSL/TLS Cipher Suites	SCA Cipher Suites
SSL_RSA_WITH_NULL_MD5	NULL- MD5
SSL_RSA_WITH_NULL_SHA	NULL- SHA
SSL_RSA_EXPORT_WITH_RC4_40_MD5	EXP- ARC4- MD5
SSL_RSA_WITH_RC4_128_MD5	ARC4- MD5
SSL_RSA_WITH_RC4_128_SHA	ARC4- SHA
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP- DES- CBC- SHA
SSL_RSA_WITH_DES_CBC_SHA	DES- CBC- SHA

SSL_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
-------------------------------	--------------

TLS Version 1.0 Suites

SSL/TLS Cipher Suites	SCA Cipher Suites
TLS_RSA_WITH_NULL_MD5	NULL-MD5
TLS_RSA_WITH_NULL_SHA	NULL-SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	EXP-ARC4-MD5
TLS_RSA_WITH_RC4_128_MD5	ARC4-MD5
TLS_RSA_WITH_RC4_128_SHA	ARC4-SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA
TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
-------------------------------	--------------

Additional Export 1024 and Other Cipher Suites

These ciphers can also be used with SSL Version 3.0.

SSL/TLS Cipher Suites	SCA Cipher Suites
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DES-CBC-SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_MD5	EXP1024-ARC4-MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	EXP1024-ARC4-SHA
TLS_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5	EXP1024-ARC2-CBC-MD5

Related Information

- [Cisco SCA 11000 Series Secure Content Accelerators](#)

- [Technical Support - Cisco Systems](#)
-

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 1992-2006 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).