



Configuring IKE Extended Authentication

This feature module describes the Internet Key Exchange (IKE) Extended Authentication feature. It includes information on the benefits of the new feature, supported platforms, related documents, and so forth.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 3
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 5
- Configuration Examples, page 7
- Command Reference, page 8
- Glossary, page 11

Feature Overview

IKE Extended Authentication (Xauth) is a draft RFC developed by the Internet Engineering Task Force (IETF) based on the Internet Key Exchange (IKE) protocol. The Xauth feature is an enhancement to the existing Internet Key Exchange (IKE) Protocol feature. Xauth allows all Cisco IOS software AAA authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. The AAA configuration list-name must match the Xauth configuration list-name for user authentication to occur.

The Xauth feature is an extension to the IKE feature, and does not replace IKE authentication.

Benefits

Additional Security

Before Xauth, IKE only supported authentication of the device, not authentication of the user using the device. With Xauth, IKE can now authenticate the user using the device after the device has been authenticated during normal IKE authentication, using any of the Cisco IOS software AAA authentication methods.

Restrictions

Enhancement to IKE

Xauth does not replace IKE. While IKE allows for device authentication, Xauth allows for user authentication. This Xauth user authentication occurs after IKE device authentication. Xauth occurs after IKE authentication phase 1, but before IKE IPSec SA negotiation phase 2.

Strong Encryption Limitations

Cisco IOS software images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to United States government export controls, and have a limited distribution. Images to be installed outside the United States require an export license. Customer orders might be denied or subject to delay due to United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

Related Features and Technologies

The *IKE Extended Authentication* feature module is related to the following existing features:

- Authentication, authorization, and accounting (AAA) feature—This feature is available in the *Cisco IOS Security Configuration Guide*, Release 12.1 and the *Cisco IOS Security Command Reference*, Release 12.1.
- IP Security Protocol (IPSec) feature—This feature is available in the *Cisco IOS Security Configuration Guide*, Release 12.1 and the *Cisco IOS Security Command Reference*, Release 12.1.
- Internet Key Exchange Protocol (IKE) feature—This feature is available in the *Cisco IOS Security Configuration Guide*, Release 12.1 and the *Cisco IOS Security Command Reference*, Release 12.1.
- Wildcard Pre-shared Key Enhancement feature—This feature is available as a new feature for Cisco IOS Release 12.1(1)T.
- IKE Shared Secret from AAA feature—This feature is available as a new feature for Cisco IOS Release 12.1(1)T.

Related Documents

For information related to the Xauth feature, refer to the following documents:

- *Cisco IOS Security Configuration Guide*, Release 12.1
- *Cisco IOS Security Command Reference*, Release 12.1
- Cisco Secure VPN Client Version 1.1 documents
- Cisco Secure PIX Firewall Version 5.1 documents
- *Wildcard Pre-shared Key Enhancement* feature module
- *IKE Shared Secret from AAA* feature module
- *IETF Extended Authentication Draft*, draft-ietf-ipsec-isakmp-xauth-04.txt



Note

Cisco Secure VPN Client Version 1.1 and Cisco Secure PIX Firewall Version 5.1 are currently based on Xauth revision 3. These products will support the current version of Xauth at a later date.

Supported Platforms

- Cisco 800 series
- Cisco 1600 series
- Cisco 1700 series (Cisco 1720 VPN, Cisco 1750)
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
- Cisco AS5300 universal access servers
- Cisco MC3810 multiservice access concentrators
- Cisco 7000 family (Cisco 7100 VPN series, 7200 series, and Cisco 7500 series)

The Xauth feature is supported on all platforms that support IPsec in Cisco IOS Release 12.1 T.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

For descriptions of supported MIBs and how to use MIBs, see Cisco's MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

IETF Extended Authentication Draft, draft-ietf-ipsec-isakmp-xauth-04.txt

Prerequisites

IPsec Software Image Required

Before configuring the Xauth feature, you must have an encryption software image that supports the Xauth feature downloaded on to your router. For more information on downloading a software image, see the following publications:

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.1
- *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.1

Authentication Configuration Required

Before configuring Xauth, you must set up an authentication list using AAA commands.

Command	Purpose
Router(config)# aaa authentication login {default list-name} method1 [method2...]	Set the AAA authentication at login.

For more information on configuring AAA commands, see the following publications:

- “Authentication, Authorization, and Accounting (AAA)” section of the *Cisco IOS Security Configuration Guide*, Release 12.1
- “Authentication, Authorization, and Accounting (AAA)” section of the *Cisco IOS Security Command Reference*, Release 12.1

IPSec and IKE Configuration Required

Before configuring Xauth, you must configure an IPSec transform, a crypto map, and ISAKMP policy using IPSec and IKE commands.

Command	Purpose
Router(config)# crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]	Define a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.
Router(cfg-crypto-trans)# mode [tunnel transport]	Specify the mode for the transform set.
Router(cfg-crypto-trans)# exit	Exit crypto transform configuration mode.
Router(config)# crypto map map-name seq-num ipsec-isakmp	Create or modify a static crypto map entry, and enters the crypto map configuration mode.
Router(config-crypto-map)# match address [access-list-id name]	Specify an extended access list for a crypto map entry.
Router(config-crypto-map)# set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]	Specify which transform sets can be used with the static crypto map entry.
Router(config-crypto-map)# exit	Exit crypto map configuration mode.
Router(config)# crypto isakmp policy priority	Define an IKE policy, and enters ISAKMP policy configuration mode.
Router(config-isakmp)# hash {sha md5}	Specify the hash algorithm within an IKE policy.
Router(config-isakmp)# authentication {rsa-sig rsa-encr pre-share}	Specify the authentication method within an IKE policy.
Router(config-isakmp)# exit	Exit ISAKMP policy configuration mode.

Command	Purpose
Router(config-crypto-map)# crypto map <i>map-name seq-num ipsec-isakmp dynamic dynamic-map-name</i>	Create or modify a dynamic crypto map entry, and enters the crypto map configuration mode.
Router(config-crypto-map)# set transform-set <i>transform-set-name1 [transform-set-name2...transform-set-name6]</i>	Specify which transform sets can be used with the dynamic crypto map entry.
Router(config-crypto-map)# exit	Exit crypto map configuration mode.
Router(config)# crypto isakmp key <i>keystring address peer-address</i>	Configure a pre-shared authentication key.
Router(config)# interface <i>interface</i>	Enter the interface configuration mode.
Router(config-if)# ip address <i>ip-address</i>	Indicate an IP address for the interface.
Router(config-if)# interface <i>interface</i>	Apply a previously defined crypto map to the interface.
Router(config-if)# exit	Exit interface configuration mode.

For more information on configuring IPsec and IKE commands, see the following publications:

- “IP Security and Encryption” section of the *Cisco IOS Security Configuration Guide*, Release 12.1
- “IP Security and Encryption” section of the *Cisco IOS Security Command Reference*, Release 12.1

Xauth Configuration

The Xauth configuration command is optional and is disabled by default.

Configuration Tasks

See the following sections for Xauth configuration tasks. Each task in the list indicates if it is optional or required:

- Configuring IKE Extended Authentication (Required)
- Verifying IKE Extended Authentication (Optional)
- Troubleshooting IKE Extended Authentication (Optional)

Configuring IKE Extended Authentication

To enable and configure a router for Xauth, perform the following tasks beginning in crypto map configuration mode:

- Configuring AAA (Required)
- Configuring IPsec Transform (Required)
- Configuring Static Crypto Map (Required)
- Configuring Xauth (Required)
- Configuring ISAKMP Policy (Required)
- Configuring Dynamic Crypto Map (Optional)



Note

For information on configuring AAA, IPsec transform, static crypto map, ISAKMP policy, and dynamic crypto map, see “Prerequisites.”

Command	Purpose
Router(config)# crypto map <i>map-name</i> client authentication list <i>list-name</i>	(Required) Enable extended authentication on a crypto map.

Verifying IKE Extended Authentication

To verify that the Xauth is enabled, enter the **show crypto map** command at the EXEC prompt. If the **crypto map client authentication list** command does not appear in the crypto map output, then Xauth is not enabled.

Troubleshooting IKE Extended Authentication

Enter the following debug commands in EXEC mode to troubleshoot Xauth:

Command	Purpose
debug crypto isakmp	Display messages about IKE events
debug aaa authentication	Display information on AAA/Terminal Access Controller Access Control System Plus (TACACS+) authentication.
debug tacacs	Display information associated with the Terminal Access Controller Access Control System (TACACS).
debug radius	Display information associated with the Remote Authentication Dial-In User Server (RADIUS)

Configuration Examples

Example 1 *Configuring Xauth with Static Crypto Map*

In the following example output from the **show running configuration** global configuration command, Xauth is configured with IKE pre-shared key using AAA local policy:

```
aaa new-model
aaa authentication login xauthlist local
!
username robin password cisco1234
!
crypto ipsec transform-set xauthtransform esp-des esp-md5-hmac
!
crypto isakmp policy 1
  hash md5
  authentication pre-share
crypto isakmp key cisco1234 address 209.165.202.145
!
crypto map xauthmap client authentication list xauthlist
crypto map xauthmap 10 ipsec-isakmp
  set peer 209.165.202.145
  set transform-set xauthtransform
  match address 192
!
interface Ethernet1/0
  ip address 209.165.202.147 255.255.255.224
  crypto map xauthmap
!
access-list 192 permit ip host 209.165.202.147 host 209.165.202.145
```

Example 2 *Configuring Xauth with Dynamic Crypto Map*

In the following example output from the **show running configuration** global configuration command, a corporate gateway uses Xauth configured on a RADIUS authentication server. Digital certification is also configured with dynamic crypto maps for scalability. This allows for both remote user authentication and device authentication.

```

aaa new-model
radius-server host alcatraz
radius-server key cisco12345
aaa authentication login xauthlist radius
!
crypto ipsec transform-set remote esp-des esp-md5-hmac
!
crypto ca identity myca
  enrollment url http://myca.cisco.com:80
crypto ca certificate chain myca
  certificate ca <cert-serial-number>
  <hex data>
  certificate
  <hex data>
!
crypto dynamic-map xauthdynamic 10
  set transform-set xauthtransform
!
crypto map xauthmap client authentication list xauthlist
crypto map xauthmap 10 ipsec-isakmp dynamic xauthdynamic
!
interface Ethernet1/0
  ip address 209.165.202.147 255.255.255.224
  crypto map xauthmap

```

Command Reference

This section documents a new command, **crypto map client authentication list** global configuration command. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

crypto map client authentication list

To configure IKE extended authentication (Xauth) on your router, use the **crypto map client authentication list** global configuration command. Use the **no** form of this command to restore the default value.

[no] crypto map *map-name* **client authentication list** *list-name*

Syntax Description		
	<i>map-name</i>	The name you assign to the crypto map set.
	<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in. The list-name must match the list-name defined during AAA configuration.

Defaults Xauth is not enabled.

Command Modes Global configuration mode

Command History	Release	Modification
	12.1(1)T	This command was introduced in Cisco IOS Release 12.1 T.

Usage Guidelines

Before configuring Xauth, you should set up an authentication list using AAA commands.

Before configuring Xauth, you should configure an IPSec transform, a crypto map, and ISAKMP policy using IPSec and IKE commands.

After enabling Xauth, you should apply the crypto map on which Xauth is configured to the router interface.

Examples The following example configures user authentication (a list of authentication methods called *xauthlist*) on an existing static crypto map called *xauthmap*:

```
crypto map xauthmap client authentication list xauthlist
```

The following example configures user authentication (a list of authentication methods called *xauthlist*) on a dynamic crypto map called *xauthdynamic* that has been applied to a static crypto map called *xauthmap*:

```
crypto map xauthmap client authentication list xauthlist
crypto map xauthmap 10 ipsec-isakmp dynamic xauthdynamic
```

Related Commands	Command	Description
	aaa authentication login	Set AAA authentication at login.
	crypto ipsec transform-set	Define a transform set, which is an acceptable combination of security protocols and algorithms, and enters crypto transform configuration mode.
	crypto map (global configuration)	Create or modify a crypto map entry, and enters the crypto map configuration mode
	crypto isakmp policy	Define an IKE policy, and enters ISAKMP policy configuration mode.
	crypto isakmp key	Configure a pre-shared authentication key.
	interface	Enter the interface configuration mode.

Glossary

AAA—authentication, authorization, and accounting. A framework of security services that provide the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

authentication—The method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption. Authentication establishes data integrity and ensures no one tampers with the data in transit. It also provides data origin authentication.

authentication, authorization, and accounting—See AAA.

IKE—A key management protocol standard which is used in conjunction with the IPsec standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is a hybrid protocol which implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.)

Internet Key Exchange—See IKE.

IP Security Protocol—See IPsec.

IPsec—IP Security Protocol. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

pre-shared key—A pre-shared key is a shared secret that is used during IKE authentication.

TACACS+—Terminal Access Controller Access Control System Plus. A security protocol that provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through authentication, authorization, and accounting (AAA) and can be enabled only through AAA commands.

Terminal Access Controller Access Control System Plus—See TACACS+.

RADIUS—Remote Authentication Dial-In User Service. A distributed client/server system that secures networks against unauthorized access. RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

Remote Authentication Dial-In User Service—See RADIUS.

SA—security association. An instance of security policy and keying material applied to a data flow. Both IKE and IPsec use SAs, although SAs are independent of one another. IPsec SAs are unidirectional and they are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPsec SA, it is bi-directional. IKE negotiates and establishes SAs on behalf of IPsec. A user can also establish IPsec SAs manually.

A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports ESP between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPsec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

security association—See SA.

Virtual Private Network—See VPN.

VPN—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunnels to encrypt all information at the IP level.