

# When Is PPTP Encryption Supported on a Cisco VPN 3000 Concentrator?

Document ID: 5754

---

- Introduction**
- Before You Begin**
  - Conventions
  - Prerequisites
  - Components Used
- PPTP Requirements**
  - Notes
- Related Information**

---

## Introduction

The Cisco VPN 3000 Concentrator can authenticate client connections through multiple methods. On the VPN 3000 Client, encryption and authentication are independent from one another. Therefore, the Cisco VPN Client can use any authentication method and still encrypt data. Confusion occurs when Point-to-Point Tunnel Protocol (PPTP) client connections are also made to the same Cisco VPN 3000 Concentrator.

## Before You Begin

### Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

### Prerequisites

There are no specific prerequisites for this document.

### Components Used

The information in this document is based on the software and hardware versions below.

- Cisco VPN 3000 Concentrator Series, all releases

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.

## PPTP Requirements

PPTP requires the authentication server to return an Accepted message along with an initial session key to start encryption. Therefore the authentication server must be able to return attributes and not just an Accept or Reject message. Unfortunately, most authentication methods do not provide return attributes with a valid authentication message. You cannot use those methods if you require encrypted PPTP sessions. All authentication methods allow PPTP connections without encryption.

The following chart is a guide for PPTP client connections (with and without encryption) and the various authentication methods.

Server	PPTP (no encryption)	PPTP (with encryption)
Internal Authentication Server	Yes	Yes
RADIUS	Yes	Yes, but see Notes
SDI (Security Dynamics International) ACE Server	Yes	No
NT Domain	Yes	No

## Notes

- Many RADIUS servers do not support Microsoft Challenge Authentication Protocol version 1 (MSCHAPv1) or MSCHAPv2 user authentication. MSCHAP is *required* to do encryption with PPTP.
- Some RADIUS servers that support MSCHAP currently do not support MSCHAPv2. For PPTP clients to connect, you must uncheck **MSCHAPv2** in the **Base Group | PPTP Authentication Protocols** section of the VPN 3000 Concentrator Manager.
- To use encryption with PPTP, your RADIUS server must support MSCHAPv1 authentication and the return attributes MSCHAP-MPPE-Keys and MSCHAP-MPPE-TYPES. Some RADIUS servers that support MSCHAP-MPPE-Keys are as follows:
  - ◆ Cisco Secure ACS for Windows Release 2.6 and later
  - ◆ Funk Software Steel-Belted RADIUS
  - ◆ Microsoft Internet Authentication Server with the NT 4.0 Server Options Pack\*\*
  - ◆ Microsoft Commercial Internet System (MCIS 2.0)
  - ◆ Microsoft Windows 2000 Internet Authentication Server

\*\* There are known Microsoft 128-bit MPPE key issues with SP5 and later on Windows NT 4.0 IAS systems. See MPPE Keys Not Handled Correctly for a 128-Bit MS-CHAP Request (Q235284) for more information. The only resolution for this is to reinstall the NT 4.0 Server Option Pack without adding the Service Pack afterwards.

---

## Related Information

- [PPTP Support Page](#)
- [RFC 2637: Point-to-Point Tunneling Protocol \(PPTP\)](#)
- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3000 Series Client Support Page](#)
- [IPSec Support Page](#)
- [Technical Support – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)