

MeetingPlace Web Security FAQ

Document ID: 51069

Questions

Introduction

When the User ID and Password are passed from the desktop to the server, is HTTP Authentication, NT LAN Manager (NTLM) v2, or Kerberos used?

Is the traffic from Cisco MeetingPlace Desktop Sharing encrypted? If so, what protocol is used?

Related Information

Introduction

This document contains frequently asked questions regarding Cisco MeetingPlace Web Security.

For more information on document conventions, refer to the Conventions Used in Cisco Technical Tips.

Q. When the User ID and Password are passed from the desktop to the server, is HTTP Authentication, NT LAN Manager (NTLM) v2, or Kerberos used?

A. Cisco MeetingPlace Web is setup with Internet Information Services (IIS) to use Web Authentication (HTTP Authentication). It can also be setup with IIS to use Windows Integrated Authentication.

According to Microsoft's article, Windows Integrated Authentication uses Kerberos version 5 and NTLM authentication. The actual protocol it uses depends on the client OS platform and the client browser support of the protocol.

Many customers use the Integrated NT Authentication method. It, however, requires additional work from MeetingPlace Professional Services to create a custom start page (to remove the domain name) and to resolve case and length issues (for user names).

In all cases, the password is encrypted (shown as a hash in the IIS log), but the User ID is not. The encryption used with Web Authentication, however, is a well-known encryption algorithm and can be easily cracked. For true security, it is best to deploy Secure Socket Layer (SSL).

Q. Is the traffic from Cisco MeetingPlace Desktop Sharing encrypted? If so, what protocol is used?

A. You can install a Secure Socket Layer (SSL) certificate and conduct conferencing through the HTTPS protocol, to encrypt Cisco MeetingPlace Web Conferencing. The same SSL encryption also applies to the Cisco MeetingPlace Web Login interface.

Note: All Cisco MeetingPlace Web Conferencing packets are sent over the same channel: direct (1627), HTTP, or HTTPS. If HTTPS is not used, the packets are not encrypted.

Related Information

- **Voice Technology Support**
 - **Voice and Unified Communications Product Support**
 - **Recommended Reading: Troubleshooting Cisco IP Telephony**
 - **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.](#)

Updated: Jan 31, 2006

Document ID: 51069
