

# NTLM和LDAP身份验证有何区别？

## 目录

[问题](#)

[环境](#)

[客户体验](#)

[基本](#)

[NTLM\(SSP\)](#)

[安全](#)

[基本](#)

[NTLM\(SSP\)](#)

## 问题

NTLM和LDAP身份验证有何区别？

## 环境

思科网络安全设备(WSA)，所有AsyncOS版本

使用WSA进行身份验证可以分为以下几种可能性：

客户端 > WSA	WSA > 身份验证服务器	身份验证服务器类型
基本身份验证	LDAP 验证	LDAP 服务器
基本身份验证	LDAP 验证	使用LDAP的Active Directory服务器
基本身份验证	NTLM基本身份验证	Active Directory服务器 ( NTLM基本 )
NTLM身份验证	NTLMSSP身份验证	Active Directory服务器(NTLMSSP)

**注意：**NTLMSSP通常称为NTLM。

基本身份验证和NTLM身份验证之间的显著区别如下。

## 客户体验

### 基本

始终会提示客户端输入凭证。输入凭证后，浏览器通常会提供一个复选框来记住提供的凭证。每当

浏览器关闭时，客户端将再次提示或再次发送之前记住的凭据。

**注意：**NTLM Basic从客户端使用基本身份验证，因此具有相同的属性。

## NTLM(SSP)

- 客户端将使用其Windows登录凭证透明地进行身份验证。
- 只有当Windows凭证首次失败（如果客户端本地登录计算机而不是登录用于身份验证的域）或客户端不信任WSA时，客户端才会提示输入凭证。

## 安全

### 基本

凭证使用纯文本不安全地发送。客户端和WSA之间的简单数据包捕获将显示用户的用户名和密码。

## NTLM(SSP)

凭证通过三次握手（摘要式身份验证）安全发送。密码从不通过线路发送。

NTLM进程如下所示：

1. 客户端发送NTLM协商数据包。这会告诉WSA客户端要执行NTLM身份验证。
2. WSA向客户端发送NTLM质询字符串。
3. 客户端使用基于其密码的算法修改质询，并将质询响应发送到WSA。
4. 然后，AD服务器根据客户端是否正确修改了质询字符串来验证客户端是否使用了正确的密码。