# Auth fails through WSA when client uses NEGOEXTS

## Contents

## Introduction

This document describes how to overocme the issue when Auth fails through Cisco Web Security Appliance (WSA) when client uses NEGOEXTS.

## Background Information

The Cisco Web Security Appliance (WSA) can authenticate users to apply policies based on user or group. One of the methods that is available is Kerberos. When using Kerberos as an authentication method in an Identity, the WSA replies to a client's HTTP request with a 401 (transparent) or 407 (explicit) HTTP response that contains the header **WWW-Authenticate: Negotiate**. At this point, the client sends a new HTTP request with the **Authorization: Negotiate** header, which contains the Generic Security Service Application Program Interface (GSS-API) and Simple Protected Negotation (SPNEGO) protocols. Under SPNEGO, the user presents the **mechTypes** which it supports. These are the mechTypes that WSA supports:

- KRB5- Kerberos auth method that is used if Kerberos is supported and configured correctly on the client and if a valid Kerberos ticket is present for the service being accessed
- NTLMSSP- Microsoft NTLM Security Support Provider method that is used if no valid Kerberos tickets are available but Negotiate auth method is supported

## Problem: Auth Fails through WSA when client uses NEGOEXTS

In more recent versions of Microsoft Windows, a new auth method is supported called NegoExts, which is an extension to the Negotiate authentication protocol. This mechType is considered more secure than NTLMSSP, and is preferred by the client when the only supported methods are NEGOEXTS and NTLMSSP. More information can be found in this link:

[Introducing Extensions to the Negotiate Authentication Package](#)

This scenario typically occurs when the Negotiate auth method is selected and there is no KRB5 mechType (most likely due to missing a valid Kerberos Ticket for the WSA service). If the client selects NEGOEXTS (may be seen as NEGOEX in wireshark), then the WSA is unabled to process the auth transaction and auth fails for the client. When this occurs, these logs are seen in the auth logs:

```
14 Nov 2016 16:06:20 (GMT -0500) Warning: PROX_AUTH : 123858 : [DOMAIN]Failed to parse NTLMSSP
packet, could not extract NTLMSSP command14 Nov 2016 16:06:20 (GMT -0500) Info: PROX_AUTH :
123858 : [DOMAIN][000] 4E 45 47 4F 45 58 54 53 00 00 00 00 00 00 00 00 NEGOEXTS ........
```

When auth fails, this occurs:

If guest privileges are enabled - client is classified as **Unauthenticated** and redirected to the website

If guest privileges are disabled - client is presented with another 401 or 407 (depending on proxy method) with the remaining auth methods presented in the response header (Negotiate is not presented again). An auth prompt is likely to be occured if NTLMSSP and/or Basic auth is configured. If there are no other auth methods (Identity is configured only for Kerberos), then auth simply fails.

## Solution

The solution to this issue is to either remove Kerberos auth from the Identity -or- fix the client so that it gets a valid Kerberos ticket for the WSA service.