# SenderBase Frequently Asked Questions

## Contents

## Introduction

This document describes frequently asked questions about SenderBase.

## What is SenderBase?

The SenderBase Reputation Service (SBRS) provides an accurate, flexible way for you to reject or throttle systems suspected to be transmitting spam based on the "reputation" of the connecting IP address associated with the remote host. The SBRS returns a score based on the probability that a message from a given source is spam, ranging from -10 (certain to be spam) through 0 to +10 (certain not to be spam). Although SBRS can be used as a stand-alone anti-spam solution, it is most effective when combined with a content-based anti-spam scanner, such as Cisco Anti-Spam.

## Frequently Asked Questions

- How does SenderBase work?
- How do I use SenderBase?
- How are SBRS scores determined and what do they mean?
- What are the best practices for using SenderBase?
- Is SenderBase on the ESA another DNS RBL?
- What types of blacklists are used by SenderBase?
- Does SenderBase function correctly behind NAT?
- What does the SBRS value of 'none' mean?
- Why does the sending IP address of my ESA has a low SBRS and how can this be fixed?
- What data is sent to SenderBase and how can this be disabled?
- How do I modify the subject header to flag messages that have a low SBRS?