Authenticating SIGNiX as an HTTP/HTTPS Client

Version 1.0
November 14, 2014

Introduction

SIGNiX may make outgoing calls to a customer site, for example to do push notifications or to retrieve documents to be signed. Customers should require clients making such requests to authenticate before allowing access.

This document explains the types of client authentication that SIGNiX supports.

HTTP Client Authentication

SIGNiX supports HTTP Basic and Digest authentication in outgoing calls it makes to other sites.

SIGNiX and the site operator must agree on a user ID and password to use to access the site.

SIGNiX does not currently support realms. All requests to the same host will get the same user ID and password, regardless of the Realm.

Server Setup

To use this type of authentication, the site SIGNiX is calling must have its server configured to require one of these methods. The details of how to do this depend on the type of web server the site has. SIGNiX customers must handle this part themselves.

- **NOTE 1: HTTP Basic authentication sends passwords in the clear and is not secure. It is strongly recommended that the server require HTTPS connections if this type of client authentication is used.**
- **NOTE 2: HTTP Digest authentication sends a hash of the password and not the password itself, but uses MD5 to form the hash. MD5 is no longer considered to be very secure. This method is also vulnerable to man-in-the-middle attacks, since the client does not authenticate the server when this method is used on its own. It is therefore recommended that the server require HTTPS connections if this type of client authentication is used. HTTPS provides the missing server authentication and encrypts the weakly hashed password data.**

Testing a New Remote Site

If a remote site has a secured URL that SIGNiX can send requests to without causing a problem, SIGNiX can manually send test requests to the server to check whether the server will accept them.

SSL Client Certificates

The SIGNiX system supports SSL client authentication when it makes SSL calls as a client to other servers that require client authentication.

SIGNiX has a client certificate from a widely trusted CA. Any remote site can configure their server to use this certificate to validate SIGNiX requests. This certificate is available on request.

SIGNiX can also accommodate sites that want it to use a specific client certificate they supply. Such a certificate should be self-signed or chain to a root that is specific to the site.

Sending Test Requests to a Site

If a remote site has a URL that SIGNiX can send requests to without causing a problem, SIGNiX can manually send test requests to the server to check whether the server will accept them.