Remote Authentication for Ariba On Demand

ARIBA®

Table of Contents

Introduction

Protecting corporate information and technology assets from intruders, thieves, and vandals is a significant challenge for most enterprises. Today's global network economy is forcing organizations to be increasingly security-aware. In every Business Technographics® survey that Forrester has conducted since 2003, business and technology decision-makers have ranked security among their organizations' top four IT initiatives for the year. The core problem we face in security hasn't changed in thousands of years; we want to grant access to information and infrastructure to the people we trust, and we throw spears at everyone else. Many organizations are implementing tougher security measures, such as user authentication policies that require strong passwords and frequent password changes. Unfortunately, these policies sometimes have unexpected results. Users are burdened with more passwords to remember. The end result is frustrated users coping by reusing similar passwords across password changes or writing down passwords. Even worse, the overall level of corporate security may go down, not up.

Achieving end-user satisfaction and increased authentication security need not be contradictory goals. Remote Authentication options such as those offered by the Ariba Suite of On-Demand Solutions tackle the strong-authentication problem. End users no longer have to wrestle with multiple unique logons or contend with forgotten passwords. All Ariba solutions have the ability to integrate with an existing Single Sign-On (SSO) solution to securely authenticate users once and then move from application to application transparently without requiring them to log in again.

Remote Authentication

Overview

Remote Authentication is a session/user authentication process that allows users to access the Ariba suite of solutions using the same user id and password as their corporate identity. It can be integrated with a Single-Sign-On (SSO) solution in the enterprise so that users login just once in order to access all applications within the enterprise as well as Ariba On-Demand solutions. SSO systems store user credentials for multiple applications and automatically submit those credentials on behalf of users when needed. Users log in once, rather than re-authenticating with a separate set of credentials for each application they access. Using SSO can also provide centralized control and enforcement of corporate authentication policies.

Authentication Options

Users can log into Ariba On-Demand solutions through three possible methods:

1. **Application Authentication.** Users have Ariba On-Demand solution user ids and passwords that they manually enter on the Ariba On-Demand solution login page (the user ids and passwords are maintained by the customer administrator within the Ariba solution).
2. **Corporate Authentication.** This is a remote authentication mechanism wherein users manually log into Ariba On-Demand solutions using the same username and password as their corporate identity (this requires the Ariba solution usernames to be the same as the corporate usernames).
3. **Corporate Authentication with SSO.** This is a remote authentication mechanism wherein users simply log into their corporate network, which automatically logs them into Ariba On-Demand solutions when needed.

In order to leverage your organization's SSO solution for Ariba solutions, your network administrators need to enable communication between your user authentication systems and Ariba On-Demand solutions.

Benefits

Remote Authentication offers the following benefits over regular access:

- Convenience for users. Users do not need to remember separate usernames or passwords for their Ariba On-Demand solution accounts. If your organization uses SSO, users will be automatically authenticated for Ariba On-Demand solutions whenever they log in to your corporate network.
- Better security control. Your organization might have greater security requirements than the authentication mechanism of Ariba On-Demand solutions. For example, your corporate network policy might require more frequent password changes. Or, your network might require the use of advanced authentication devices, such as RSA SecurID® devices or fingerprint scanners.
- Better account management. When users leave your organization, their access to Ariba On-Demand solutions is automatically revoked as part of your organization's network policy. Removing their log in permission from your corporate network means that they can no longer access Ariba On-Demand solutions.

Corporate Authentication: Remote Authentication Protocols

Ariba supports two industry standards-based remote authentication protocols to enable corporate authentication (with or without SSO).

Ariba Remote Authentication Relay Protocol

The Remote Authentication Relay Protocol is a simple yet secure protocol based on industry-standard Public Key Infrastructure (PKI). It is easy to implement and does not require additional software from third-party vendors.

This protocol is:

- **Secure.** It uses Public Key Infrastructure (PKI) using RSA technology, which is an industry standard method for keeping data secure on the Internet.
- **Internet friendly.** It integrates with your corporate network infrastructure without requiring a specialized topology. You do not need to deploy special services, such as a VPN (it works with it if you already have it), a DMZ, or custom web services.
- **Compatible with all Ariba On-Demand solutions.** It works with all Ariba On-Demand solutions, such as Procure-to-Pay, Invoice and Payment, Sourcing, Contract Management, and Spend Visibility. After you set it up, you can subscribe to additional Ariba On-Demand solutions without needing to modify it.

Ariba provides sample scripts for Microsoft Internet Information Services (IIS) using Active Server Pages and for Apache using Perl; alternatively, you can write your own scripts using any scripting language of your choice.

Ariba SAML 2.0 HTTP POST Binding Protocol

Beginning with the 10s1 release, Ariba applications can support the Security Assertion Markup Language (SAML) protocol for exchanging user-identity information. Functioning as Service Providers, Ariba applications can support both Identity Provider and Service Provider initiated SAML authentication requests and responses. This capability helps align the Ariba authentication infrastructure with a widely adopted open-standard (SAML), thereby helping customers save on deployment time and cost.

Pre-requisites

The following components are required on your network to enable remote authentication:

1. **User Database.** A system that maintains a list of your corporate users and authenticates them. This authentication can use any technology, such as LDAP or Microsoft Domain Controller.
2. **A Web Server.** A web-server that accepts HTTP connections from users' browsers.
3. **Cookies:** User's browser must allow first-party cookies.

Single Sign-On

Ariba does not bundle an SSO product with its solutions, and responsibility for the implementation of any SSO solution on the customer sides rests solely with the customer. Ariba provides assistance in integrating your existing SSO solution to work with its On-Demand offerings by loading the requisite parameters that you provide to us into your site, and switching them on for testing purposes.

If your organization does not currently have an SSO solution but is considering one, there are several options that range from:

- IIS Web Authentication for Windows: This is a low-cost alternative to a full-fledged SSO solution if your organization meets the following criteria:
  - All users use IE Browser only
  - All users are in the same NT domain as where the IIS web server is
  - All users can access this IIS web server without going through a proxy server

For configuration details, please refer to Microsoft's knowledgebase article: *http://support.microsoft.com/kb/324276/en-us*

… All the way to:

- **Enterprise SSO Solutions:** They provide complete identity management for all the users in your organization. Examples include SiteMinder from CA or WebSeal from IBM.

The above is only provided as guidance. Please check with your IT department regarding the options available within your enterprise.

Limitations

There are a few limitations in using the Remote Authentication mechanism:

- Supplier organizations cannot use Remote Authentication; it is only for buying organizations.
- Users must have access to your corporate authentication mechanism, which typically means they must have approved access to your network.
- After Corporate Authentication is turned on for your organization—your users can no longer log directly into Ariba On-Demand solutions; they must use your authentication mechanism.
- Lastly, you must continue to manage user profiles within the Ariba On-Demand solution. Each user must be a valid user within the solution for login to succeed.

Data Needed by Ariba

Ariba requires certain information about your environment to enable Remote Authentication:

1. Your public RSA key if you use Ariba Remote Relay Authentication Protocol or your public certificate if you use Ariba SAML 2.0 HTTP Post binding protocol.
2. The URL of your Remote Authentication Relay page
3. The URL of a "Logout Page," which is the page you want users to see after their sessions end

Deployment Options

Ariba Remote Authentication Relay Protocol

Overview

The Remote Authentication Relay protocol uses your existing corporate network protection mechanisms (such as IIS basic authentication or a third-party single sign-on system) to authenticate users when they want to use an Ariba On-Demand solution. The protocol uses web browser redirects to communicate between Ariba On-Demand solutions and your network authenticator.

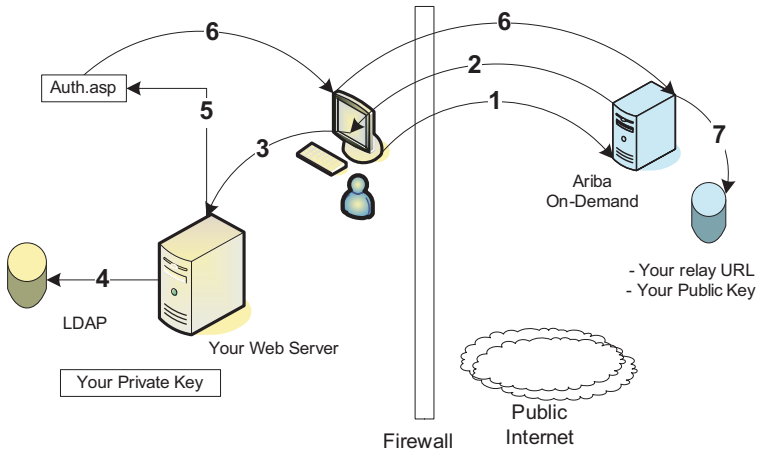
The protocol uses a relay page on your network that you protect with the authentication mechanism of your choice. Ariba does not need to know anything about your authentication mechanism or your company user directory – these decisions are left to you. If your authentication mechanism allows a user to access your relay page, Ariba allows that user to access Ariba On-Demand solutions.

Set up flow:

1. You install a relay page in your corporate web server and protect it with an authentication mechanism of your choice.
2. You generate a public/private key pair; the exact procedure is described later.
3. You send Ariba your public key, the URL of your relay page, and the URL of your "Logout Page."

Corporate Authentication: Basic

The following figures illustrate the various usage flows for the basic corporate authentication setup.

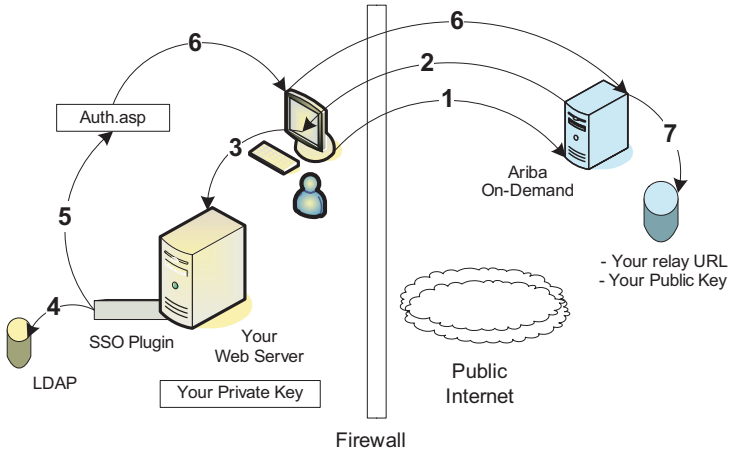


Flow with basic corporate authentication:

1. A user accesses the URL of an Ariba On-Demand solution.
2. The Ariba On-Demand solution notices that your organization is configured for Corporate Authentication and, instead of displaying a login page, it redirects the user to your relay page (Auth.asp), passing a randomly generated challenge key and a return URL. The challenge key is stored in the session during this interaction.
3. Your authentication mechanism (such as an IIS web server with basic authentication) intercepts the request from the Ariba On-Demand solution.
4. Your authentication mechanism checks the user against your user database (such as Active Directory). If authentication succeeds, your authentication mechanism forwards the request to your relay page.
5. Your relay page (auth.asp) receives the request from your authentication mechanism. It first verifies that the request is coming from the ariba.com domain. Then, it concatenates the challenge key and the username and signs the result (SHA1+RSA) with your private key. It then base64 encodes this signature. Lastly, if the relay page uses HTTP GET with the return URL, then the signature is URL encoded.
6. Your relay page sends the username and signature back to the Ariba On-Demand solution, using the return URL.
7. The Ariba On-Demand solution finds the session based on the session cookie in user's browser, retrieves the challenge key from the session, concatenates the challenge key and username and verifies the signature with its copy of your public key. A match indicates that the user is authenticated. The Ariba On-Demand solution then completes the login process as if the user had successfully entered a username and password on its login page. A failure in the process will display a proper error page and generate an audit record for debugging.

Corporate Authentication: with SSO

The following figures illustrate Corporate Authentication usage flows with SSO and IIS authentication.



1. A user accesses the URL of an Ariba On-Demand solution.
2. The Ariba On-Demand solution notices that your organization is configured for Corporate Authentication and, instead of displaying a login page, it redirects the user to your relay page (Auth.asp), passing a randomly generated challenge key and a return URL.
3. The SSO Plug-in running in your corporate web server intercepts the access to the protected relay page and checks for an existing SSO cookie. If the cookie does not exist (the user has not logged in), it redirects the user to your SSO authenticator, which displays your corporate login page.
4. The user enters authentication information and the SSO Plug-in checks it against your user database (such as Active Directory). If authentication succeeds, the SSO Plug-in forwards the original request to your relay page.
5. Your relay page (auth.asp) receives the request from your authentication mechanism. It first verifies that the request is coming from the ariba.com domain. Then, it concatenates the challenge key and the username and signs the result (SHA1+RSA) with your private key. It then base64 encodes this signature. Lastly, if the relay page uses HTTP GET with the return URL, then the signature is URL encoded.
6. Your relay page sends the signature back to the On-Demand solution, using the return URL.
7. The Ariba On-Demand solution finds the session based on the session cookie in user's browser, retrieves the challenge key from the session, concatenates the challenge key and username and verifies the signature with its copy of your public key. A match indicates that the user is authenticated. The Ariba On-Demand solution then completes the login process as if the user had successfully entered a username and password on its login page. A failure in the process will display a proper error page and generate an audit record for debugging.

Logout Page

When users finish their sessions, they click a Logout button in the Ariba On-Demand solution, which redirects them to your Logout Page. The Logout Page can be any URL you determine, such as the home page on your intranet.

Typically, you would not log users out from your network. However, you might require your corporate authenticator to log users out of your network when they log out of the Ariba On-Demand solution. In this case, provide a Logout Page URL that activates a script that logs users out of your corporate authenticator and redirects them to a final page.

Non-Authorized Users

If your authentication mechanism determines that a user is not authorized, your relay page displays either an error page or a login page. It does not forward the request to the Ariba On-Demand solution.

Implementations of the Protocol

The Remote Authentication Relay protocol offers flexible deployment options to suit your enterprise requirements:

1. **ASP:** This utilizes a combination of Microsoft Active Server Page technology and Open SSL.
2. **Perl:** This utilizes Perl scripting language and Open SSL.
3. **Java:** This option employs a Java Servlet based solution together with the Java Security Package.

For further questions on remote authentication, please contact your Ariba representative(s); you can also request them for a copy of the Ariba Remote Authentication Deployment Guide.

Ariba SAML 2.0 HTTP POST Binding Protocol

Overview

Security Assertion Markup Language (SAML) is an XML standard for exchanging authentication and authorization data between security domains. SAML is a standard set by the OASIS Security Services Technical Committee. SAML 2.0 was ratified as an OASIS Standard in March 2005. For an overview of this protocol and additional references, please visit: http://en.wikipedia.org/wiki/SAML_2.0

Ariba supports both SAML 1.1 and SAML 2.0 style SAML HTTP POST binding authentication protocols. However, note that the application specific user permissions must still be configured within the individual applications.

Corporate Authentication with SAML

SAML 1.1 with Service Provider Initiated Request

To use SAML protocol, Ariba does not need to know anything about your authentication mechanism or your company user directory. As long as your authentication mechanism is configured to allow a user to access your corporate resources over HTTP, Ariba can allow that user to access Ariba On-Demand solutions.

Configuration steps:

1. You install a resource page in your corporate web server and protect it with the SAML authentication service.
2. You provide Ariba your public certificate, your resource page URL, and your logout page URL.
3. Ariba provides you a return URL for posting SAMLResponse.

Step by step authentication flow:

1. A user accesses the URL of an Ariba On-Demand solution.
2. The Ariba On-Demand solution notices that your organization is configured for Remote Authentication and, instead of displaying a login page, it redirects the user to your resource page, passing, as an optional parameter, a service provider id. Other relevant information such as the Ariba landing page (after login) will be stored in the session details for this interaction.
3. Your SAML authentication service intercepts the request from the Ariba On-Demand solution.
4. The SAML authentication service checks the user against your user database. If authentication succeeds, it prepares a SAMLResponse document.
5. Your authentication service posts the SAMLResponse document to the URL provided by Ariba.
6. The Ariba On-Demand solution verifies the signature in the SAMLResponse document and retrieves the user information from the document. The Ariba On-Demand solution then completes the login process as if the user had successfully entered a username and password on its login page. A failure will display a proper error page and generate an audit record.

SAML 2.0 with Service Provider Initiated Request

The only difference is that the initial request from Ariba will be in the form of a SAMLRequest document instead of a redirect.

For further questions on remote authentication, please contact your Ariba representative(s); you can also request of them a copy of the Ariba Remote Authentication Deployment Guide.