

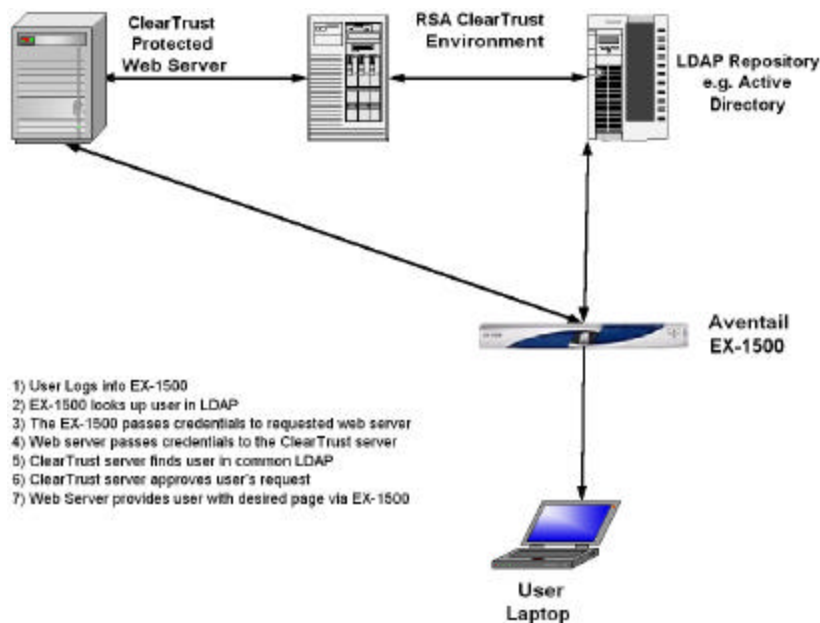


# RSA ClearTrust Ready Implementation Guide For Portal Servers and Web-Based Applications

Last Modified 9/30/03

## 1. Partner Information

Partner Name	Aventail Corporation
Web Site	<a href="http://www.aventail.com">www.aventail.com</a>
Product Name	EX-1500
Version & Platform	6.4
Product Description	<i>The EX-1500 is an SSL VPN appliance. It allows organizations to provide employees, partners and customers personalized access to corporate files, email, web applications and client/server applications.</i>
Product Category	Web Services



## 2. Contact Information

	Sales contact	Support Contact
Email	<a href="mailto:sales@aventail.com">sales@aventail.com</a>	<a href="mailto:aventailcustomerservice@aventail.com">aventailcustomerservice@aventail.com</a>
Phone	206.215.1111	206.215.0078
Web	<a href="http://www.aventail.com">www.aventail.com</a>	<a href="http://www.aventail.com">www.aventail.com</a>

### 3. Solution Summary

Feature	Details
Use UserID for SSO	Yes
Use UserID for Personalization	Yes
Recognize Authentication Type	No
API-level Authorization Support (RuntimeAPI)	No
User Management (AdminAPI)	Yes Via Shared User Repository (LDAP)

### 4. Integration Overview

The Aventail EX-1500 provides Single Sign On to RSA ClearTrust by posting user names and passwords to the RSA ClearTrust server when a user requests a protected resource. The EX-1500 is configured to use the same LDAP data source as the RSA ClearTrust environment to ensure that the credentials will work for both environments.

### 5. Product Requirements

#### Hardware requirements

Component Name: Aventail EX-1500 (Appliance)	
Appliance	The Ex-1500 is software pre-installed and tuned on Intel hardware.

#### Software requirements

Component Name:	
Operating System	Version (Patch-level)
Linux based appliance	6.4

#### Integration Modules

File Name	Destination
Aventail SSO Adapter	Consult with your Aventail Sales Engineer about applying the adapter to your EX-1500

## 6. Product Configuration

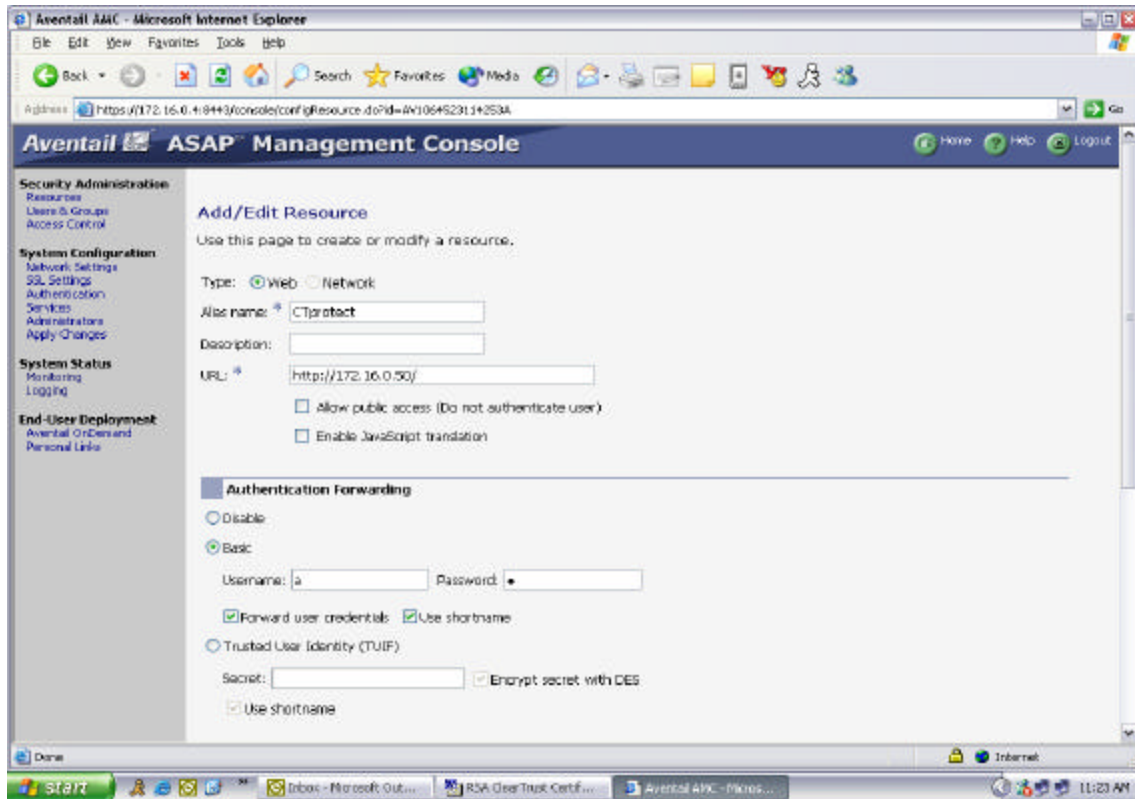
The Aventail EX-1500 must be configured to use the same LDAP repository as the RSA ClearTrust environment. LDAP is configured from the Aventail Management Console. <https://<machine-name>:8443/console>.

User integration between RSA ClearTrust and ActiveDirectory is easily achieved. User management can be performed by either the RSA ClearTrust AdminGUI or directly in the LDAP directory server.

When a user attempts to access a resource protected by RSA ClearTrust, the Aventail EX-1500 will forward the user's credentials to the RSA ClearTrust environment for Basic Authentication. If Aventail and RSA ClearTrust are using the same LDAP repository, the credentials will match, and the user will be logged into their desired resource without being presented with the RSA ClearTrust log in screen.

In order to add a ClearTrust protected resources to the Aventail EX-1500:

- 1) Log onto the Aventail AMC at <https://<machine-name>:8443/console>
- 2) Click on "resources".
- 3) Click the "Add" button.
- 4) Enter an alias name for the resource.
- 5) Enter the full URL to the protected resource.
- 6) In order to enable SSO, check the "Basic" option and leave the "Forward user credentials" and "Use shortname" check boxes enabled. Enter one character into the Username and Password fields. These characters are placeholders only. The actual user name and password will be passed to the RSA ClearTrust agent on the web server.
- 7) Click OK to add the resource.
- 8) Click on the "apply changes" link in order to add the new resource to the EX-1500. SSO to this new resource is now enabled.



## 7. Certification Checklist for Portal Servers and Web-Based Apps

Date Tested: <9/18/2003>

Product	Tested Version
RSA ClearTrust	5.0.1
RSA ClearTrust Agent	3.0.1 IIS
Aventail EX-1500	6.4

Test Case	Result
<b>Product Characteristics for SSO Support</b>	
Application/Portal is web-based, and supports access by a standard HTTP-based browser	P
Application/Portal runs on Web Server Platform supported by RSA ClearTrust	N/A
Application/Portal login interface can be modified or replaced	P
Application/Portal can extract user information from RSA ClearTrust session cookie	N/A
Application/Portal can extract user information from HTTP Headers	N/A
Application/Portal can extract authentication type from RSA ClearTrust session cookie	N/A
Application/Portal can extract authentication type from HTTP Headers	P
Application/Portal can perform SSO with other RSA ClearTrust-supported Web Server	P
<b>Login - General</b>	
HTTP basic authentication	P
Forms based	P
Forms based w/ URI retention	P
<b>Login – Basic Authentication</b>	
Access Denied for unauthorized user	P
Successful login for authorized user	P
Successful recognition of identity/personalization in 3 <sup>rd</sup> Party Product	P
Successful recognition of identity/personalization after SSO with other RSA ClearTrust-supported Web Server	N/A
<b>Login –Graded Authentication</b>	
Access Denied for unauthorized user	N/A
Successful login for authorized user	N/A
Successful recognition of identity/personalization in 3 <sup>rd</sup> Party Product	N/A
Successful recognition of identity/personalization after SSO with other RSA ClearTrust-supported Web Server	N/A

JGS

\*P=Pass or Yes F=Fail N/A=Non-available function

## 8. Known Issues

The EX-1500 expects to receive a HTTP status code of 200, operation successful, when it authenticates against the ClearTrust server or it will assume that the authentication has failed.