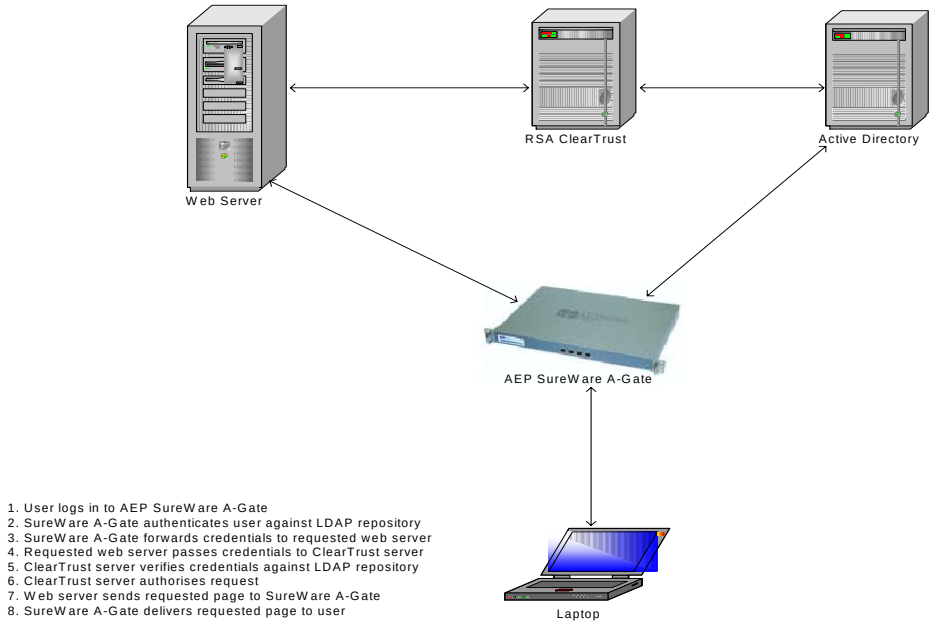
RSA ClearTrust Ready Implementation Guide
For Portal Servers and Web-Based Applications

Last Modified August 30, 2004

1. Partner Information

Partner Name	AEP Systems Ltd.
Web Site	www.aepsystems.com
Product Name	AEP SureWare A-Gate
Version & Platform	AG-600 V3.0.2
Product Description	AEP SureWare A-Gate, a suite of SSL VPN hardware appliances, provides a high functionality, low-cost SSL VPN solution for small and medium enterprises (SMEs) that want to extend enterprise applications to employees, business partners and customers. AEP SureWare A-Gate provides a full-featured solution that meets all the remote access needs of SMEs, from access to Web-enabled or Windows Terminal Services applications to full access to client-server applications. Now all remote access users - mobile employees, "road warriors", teleworkers, occasional travelers and business partners - can have secure and authenticated access to internal applications and resources.
Product Category	Remote access, Virtual Private Networking



2. Contact Information

	Sales contact	Support Contact
Email	sales@aepsystems.com	support@aepsystems.com
Phone	US/Toll Free: 800.383.7716 US/California: 650.326.6748 US/Boston: 617.790.5825 Ireland: (+353 1) 204 1300 UK: (+44) 1442 458 600	US/Toll Free: 866.443.0370 EMEA: (+353 1) 204 1300
Web	www.aepsystems.com	www.aepsystems.com

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

AEP SureWare A-Gate provides Single-Sign-On via Authentication Forwarding Rules. These rules list the servers protected by RSA ClearTrust and ensure that when a user attempts to access a resource on one of these servers, their Basic credentials are automatically forwarded with the request.

5. Product Requirements

Hardware requirements

Component Name: SureWare A-Gate AG-600	
Firmware level	3.0.2.5-ct1

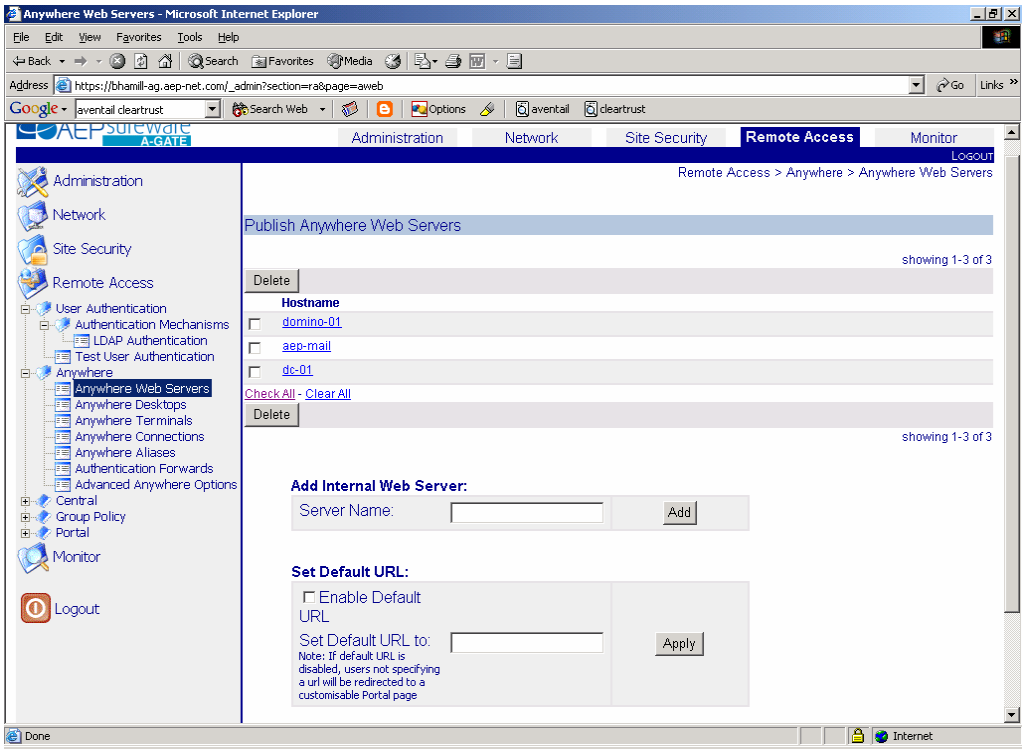
6. Product Configuration

To enable SSO perform the following steps:

- Add all ClearTrust protected servers to the 'Anywhere Web Servers' list via the A-Gate web administration interface.
- Set the HTTPS default policy to Allow.
- Configure the A-Gate to use the same LDAP repository as the RSA ClearTrust environment. Active Directory User Management can be performed either by the RSA ClearTrust AdminGUI or directly in the LDAP directory server.
- Enable LDAP Authentication.
- Create Authentication Forwards.

1. Add ClearTrust protected servers to 'Anywhere Web Servers' list via the web administration interface, https://<machine-fqdn>/_admin. A-Gate users can only access resources which reside on these configured servers.

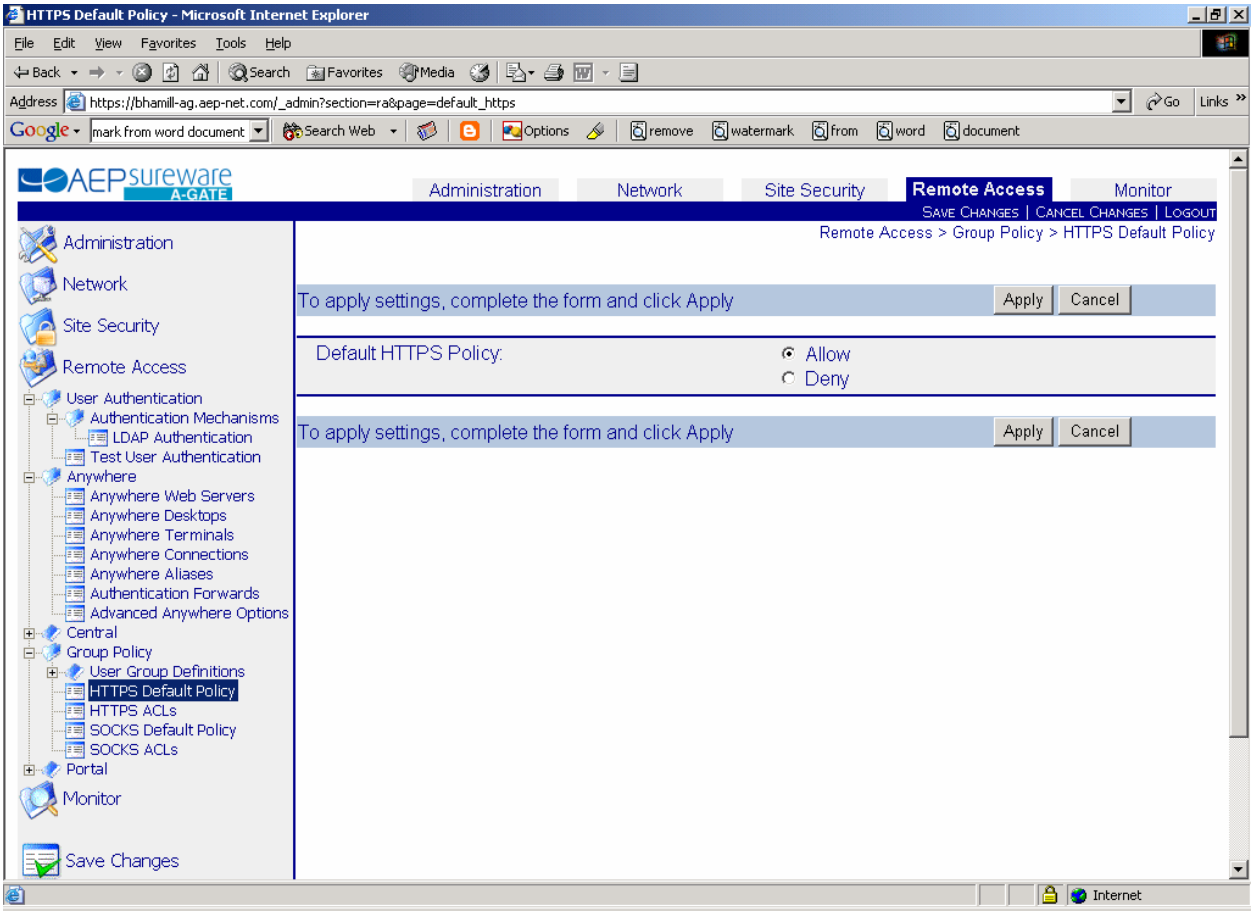
- Navigate to 'Remote Access > Anywhere > Anywhere Web Servers'.
- Enter the server name and click 'Add'.
- The new server will appear in the list at top of the page, where it can be tested for connectivity or deleted. **N.B. All ClearTrust protected servers must be added to this list.**



2. Set HTTPS default policy to ‘Allow’.

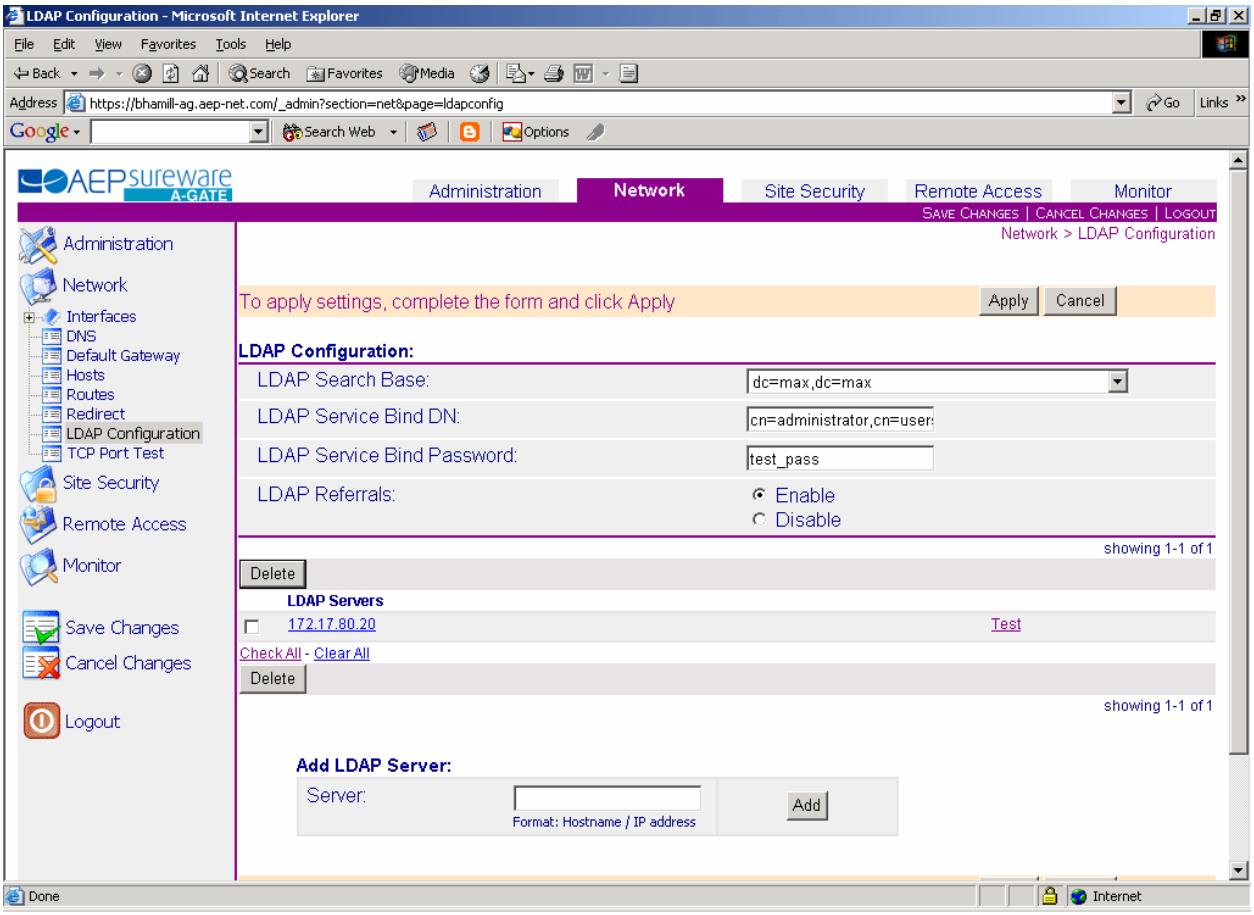
   By default, HTTPS default access policy is set to ‘Deny’, which ensures the administrator starts configuration with a secure, locked down A-Gate, where all HTTPS access requests are rejected. There are two ways to allow access to A-Gate’s back-end servers. The quickest way is to set the default HTTPS policy to ‘Allow’. The other, more controlled way is to create HTTPS ACLs. Please consult the reference manual for information on ACLs.

   - Navigate to ‘Remote Access > Group Policy > HTTPS Default Policy’.
   - Set Default Policy to ‘Allow’.
   - Click ‘Apply’.

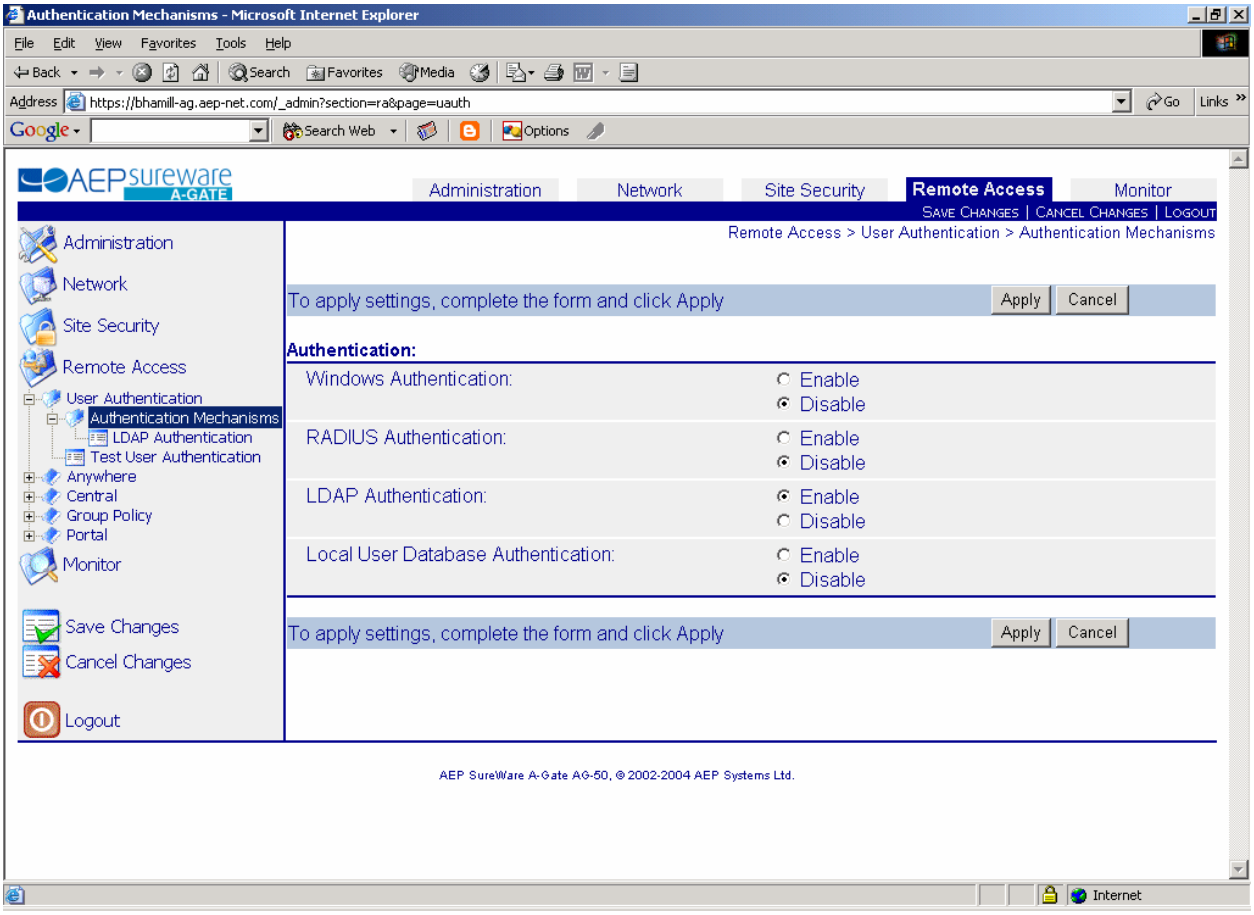


3. Configure LDAP Repository

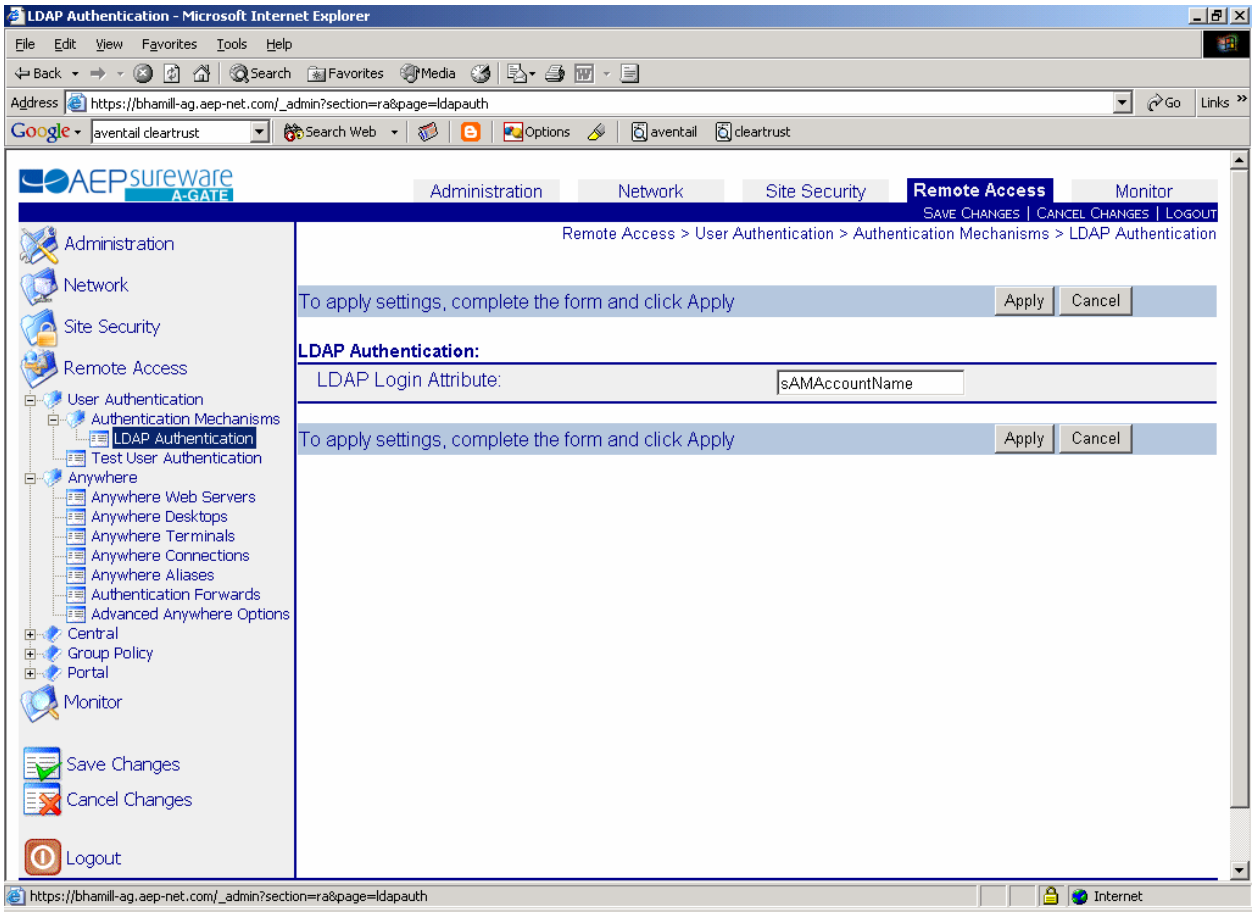
- Navigate to ‘Network > LDAP Configuration’.
- Add the Active Directory server by entering the IP address or hostname in the ‘Server:’ field of the ‘Add LDAP Server’ section.
- Click ‘Add’.
- Configure the LDAP search base (mandatory) and optionally the LDAP bind DN and password.
- Click ‘Apply’.



4. Enable LDAP Authentication
    - Navigate to ‘Remote Access > User Authentication > Authentication Mechanisms’ and select ‘Enable’ LDAP Authentication.
    - Ensure all other authentication mechanisms are disabled.
    - Click ‘Apply’.



- Navigate to ‘Remote Access > User Authentication > Authentication Mechanisms > LDAP Authentication.
- Set the ‘LDAP Login Attribute’, this should be ‘sAMAccountName’ for Active Directory.
- Click ‘Apply’.



5. Create Authentication Forwards

Single-Sign-On is achieved in the SureWare A-Gate via Authentication Forwards. This is the process whereby Basic credentials are automatically forwarded to back-end servers when requesting particular resources.

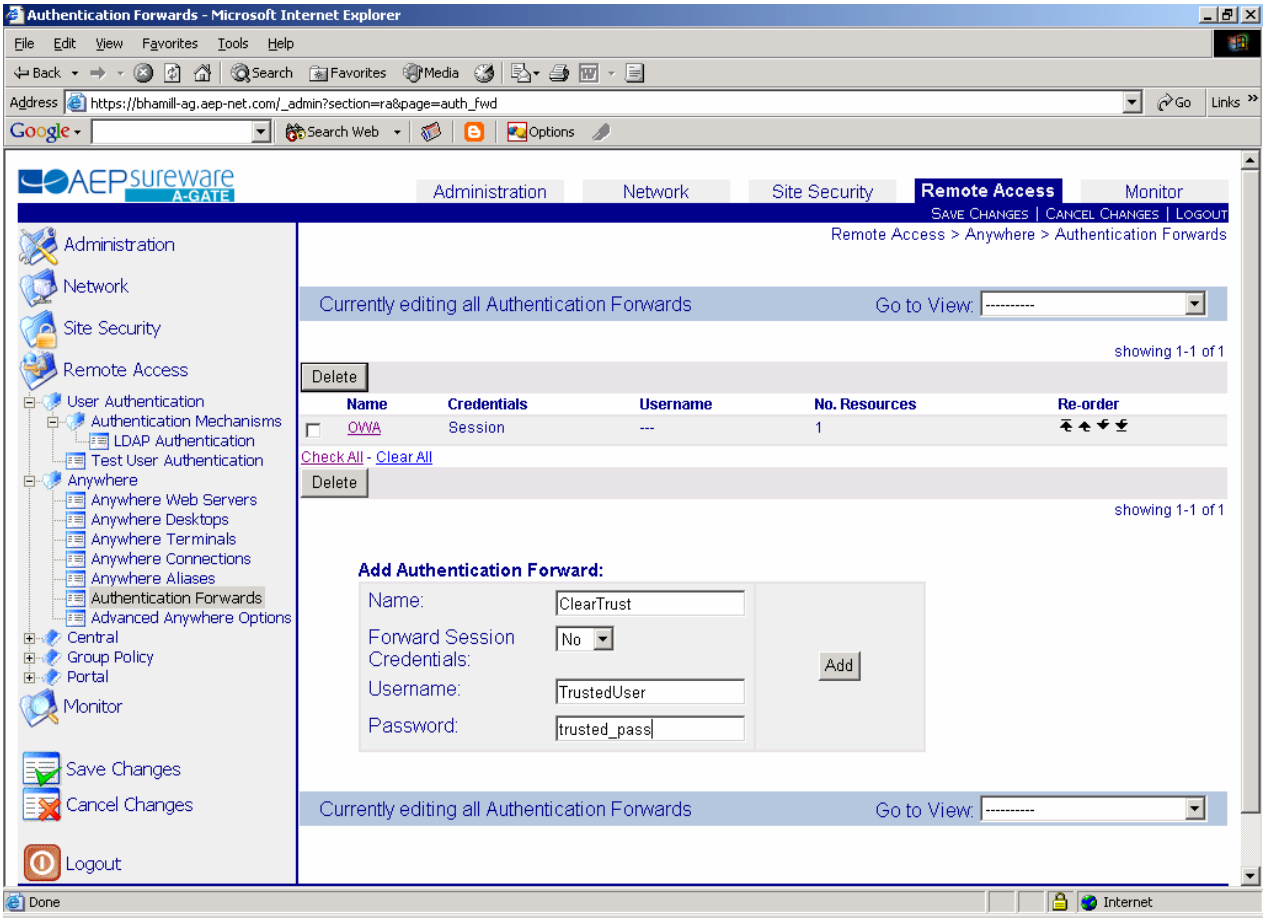
To enable this process, the administrator must create at least one Authentication Forward, consisting of a name, credentials and a list of forwarding rules which state what resources are governed by this Authentication Forward. Administrators can choose to forward the session credentials, which are the username and password entered by the user via the A-Gate Login screen, or a specific trusted username and password.

If Authentication Forwards exist, the A-Gate checks every incoming request against the list of forwarding rules. If a match occurs, the A-Gate appends an authorization header with the configured credentials to the original request and sends the request to the requested back-end server.

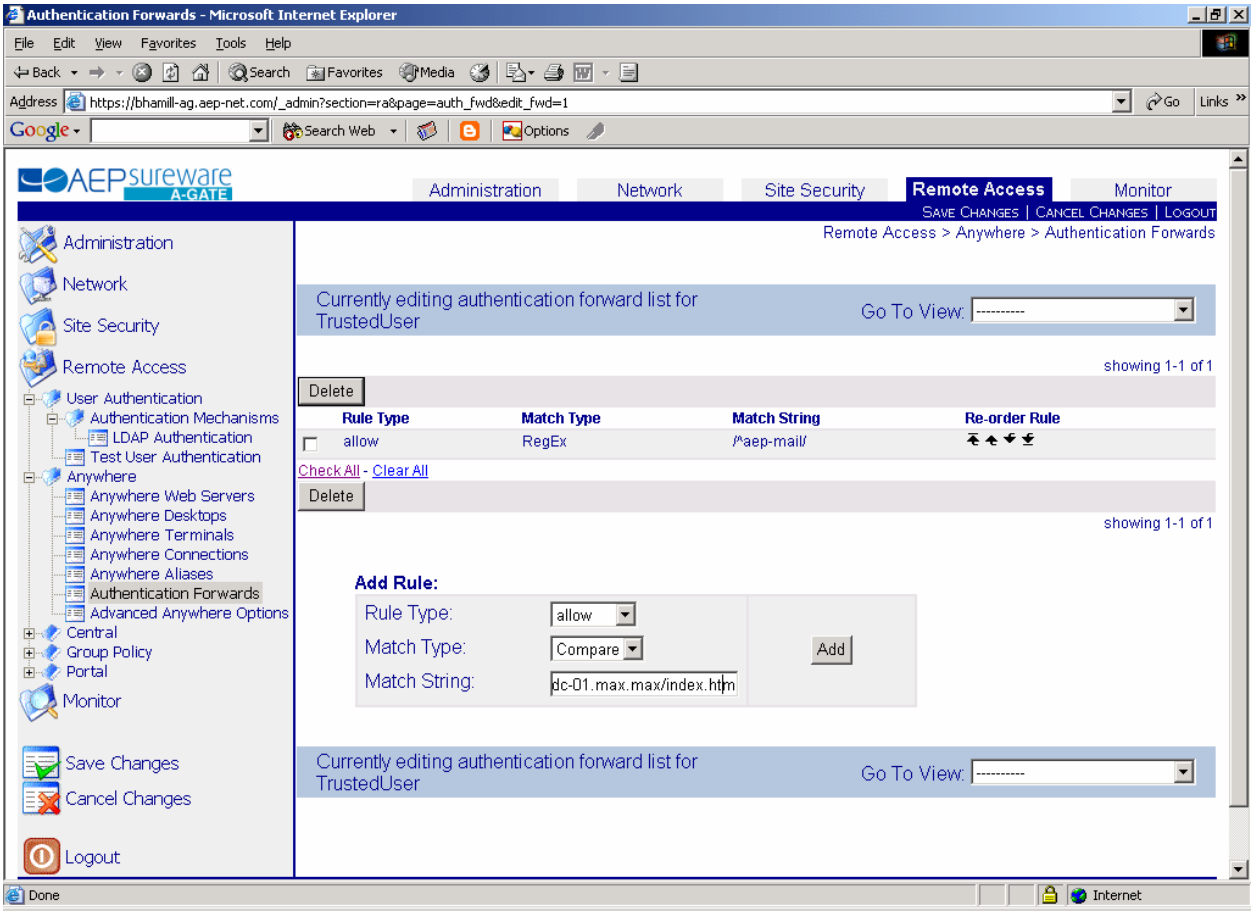
To create an authentication forward:

- Navigate to ‘Remote Access > Anywhere > Authentication Forwards’ on the web administration interface.
- Set credentials. ‘Forward Session Credentials’ determines whether or not the session credentials are forwarded to the back-end servers. If ‘No’ is selected, the administrator must enter a trusted username and password. To add this rule, click ‘Add’. The new rule will appear in the list at the

top of the page where it can be edited, deleted or re-ordered. Rule order is extremely important as the A-Gate always applies the first matching rule it encounters.



- Click on the newly created Authentication Forward to add forwarding rules.



- Each rule consists of a rule type, a match type and a match string. Rule Type indicates whether authentication forwarding is allowed, denied or required for matching resources. Match Type indicates the comparison mechanism used for this rule. Possible values are ‘Compare’ which looks for an exact match, ‘RegEx’ which matches against a regular expression or ‘Any’, which matches everything. Match String must match the requested resource if this rule is to be applied.
- Click ‘Add’ to add each rule.
- Click ‘Save Changes’ to save these rules.

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

Date Tested: August 18, 2004

Product	Tested Version
RSA ClearTrust	5.5
RSA ClearTrust Agent	4.5 IIS
AEP SureWare A-Gate	3.0.2

Test Case	Result
Product Characteristics for SSO Support	
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
Login – General	
HTTP basic authentication	P
Forms based	P
Forms based w/ URI retention	P
Login – Basic Authentication	
Access Denied for unauthorized user	P
Successful login for authorized user	P
Successful recognition of identity/personalization in 3rd Party Product	P
Successful recognition of identity/personalization after SSO with other RSA ClearTrust-supported Web Server	N/A
Login –Graded Authentication	
Access Denied for unauthorized user	N/A
Successful login for authorized user	N/A
Successful recognition of identity/personalization in 3rd Party Product	N/A
Successful recognition of identity/personalization after SSO with other RSA ClearTrust-supported Web Server	N/A

PAR/SWA

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