



BiGuard S10 SSL VPN Security Gateway

Authentication Domain

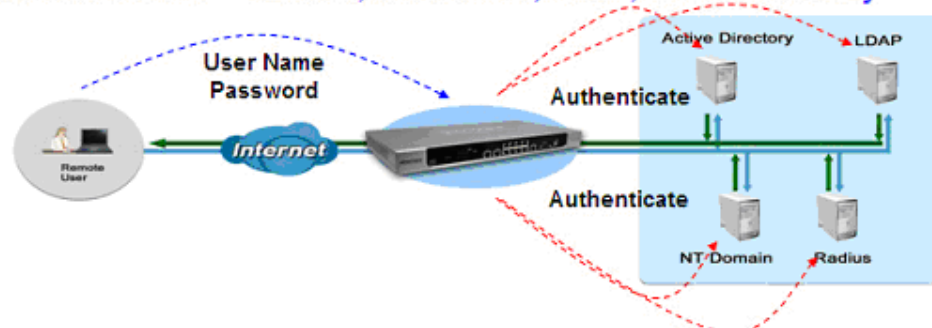
Introduction

BiGuard SSL (Secure Socket Layer) VPN (Virtual Private Network) appliances support different authentication domains to authenticate the remote user. The supported authentication domains include local user database, Active Directory, LDAP, NT Domain, and RADIUS.

The default authentication domain for BiGuard SSL VPN appliances is the local user database and the domain name is BiGuard.

Authentication Domains

Authentication Domains – RADIUS, NT Domain, LDAP, Active Directory



The BiGuardS10 and BiGuardS20 support up to 128 user names in the local user database. The local user database authentication method is the most commonly used authentication method if there is no existing authentication domain set up in your environment yet.

You will need to set up the same authentication domain to authenticate the user if the user account is already set up in an authentication domain, like Active Directory, in the company. By setting the authentication domain to authenticate the user, the user is able to log on to the SSL VPN appliances only once, and will be able to log on to the related network resources of the domain automatically when the user accesses those resources without having to type the same username/password in again.

Three Solutions in One



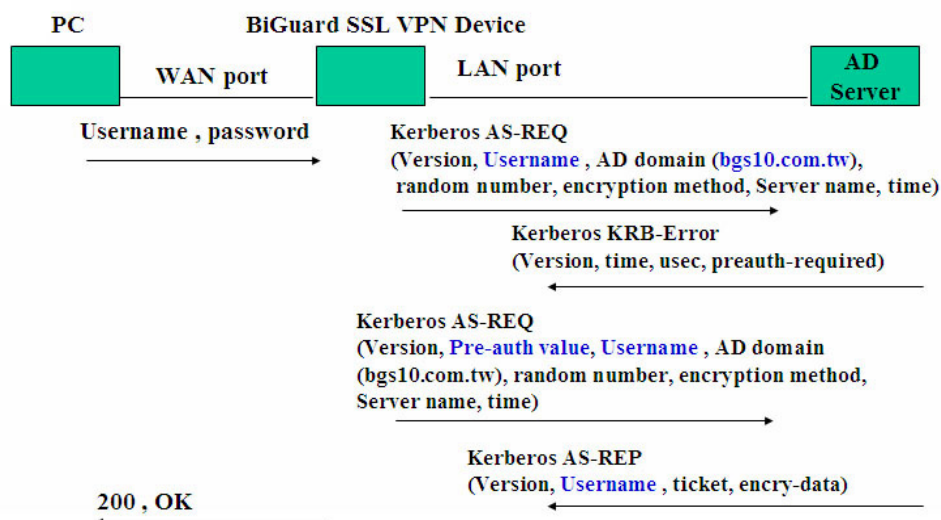
Authentication Domain Settings

Authentication Domain	BiGuard SSL VPN configuration	Web portal user input
(1) Active Directory	(1) Server IP (2) Active Directory Domain (Domain Name, e.g., bgs10.com.tw) (3) Username	(1) Username (2) Password (3) Choose Authentication Domains
(2) NT Domain	(1) Server IP (2) NT Domain Name (Domain Name, e.g., testNTDomain) (3) Username	(1) Username (2) Password (3) Choose Authentication Domains
(3) Radius	(1) Server IP (2) Server Password (3) Username	(1) Username (2) Password (3) Choose Authentication Domains
(4) LDAP	(1) Server IP (2) LDAP BaseDN (BaseDN, e.g., n=users,dc=bgs10,dc=com, dc=tw) (3) Username	(1) Username (2) Password (3) Choose Authentication Domains
(5) Local DB	(1) Username (2) Password	(1) Username (2) Password (3) Choose Authentication Domains

In the authentication domain settings list, we list the setting parameters that the administrator has to set up for the users and the parameters that users have to enter when accessing the web portal.

In the following paragraphs, we will introduce the protocol flows of each authentication domain, as this will help you understand more about the authentication process.

Active Directory (UDP, port=88)

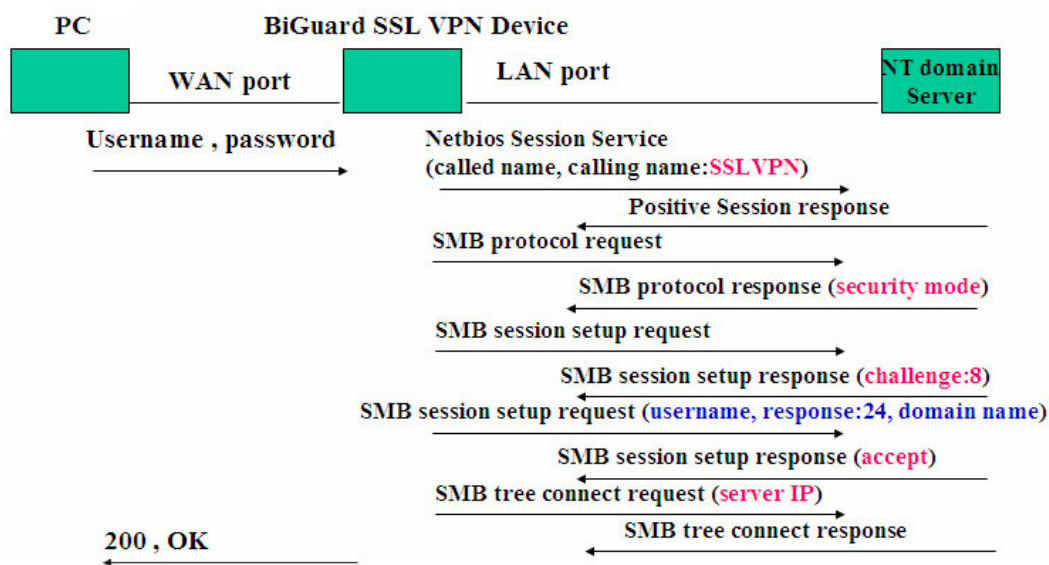


Three Solutions in One



Active Directory is based on the UDP protocol and the service port number is 88. The above diagram displays the protocol flow of Active Directory. The user from a remote site will have to enter the username and the password in order to log on to remote web portal. The BiGuard SSL VPN appliance will then look up the username entry in the configuration. If the username is found, the BiGuard SSL VPN appliance will send the username, configured domain name, encryption method, random number, server name, and time to the Active Directory server in Kerberos AS-REQ format. The Active Directory server will then reply with a Kerberos KRB-Error message with version number, time, and preauth-required as the parameters. The BiGuard SSL VPN appliances will send a Kerberos AS-REQ message with the encrypted password and other parameters to Active Directory. The Active Directory will reply with a Kerberos message with a ticket to indicate the access right of the user.

NT Domain (TCP, port=139)

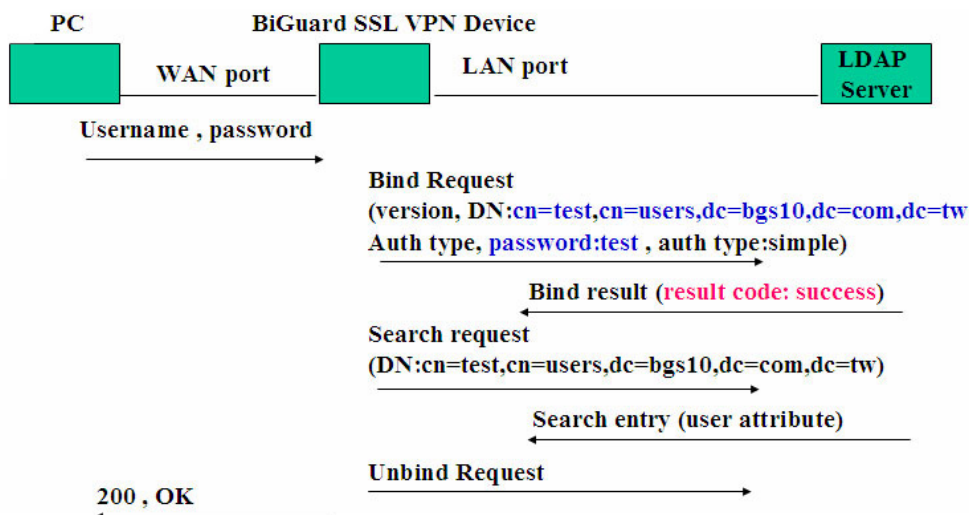


NT Domain is based on the TCP protocol and the service port number is 139. The above diagram displays the protocol flow of NT Domain authentication. The NT Domain authentication is based on SMB protocol on top of Netbios protocol.

Three Solutions in One

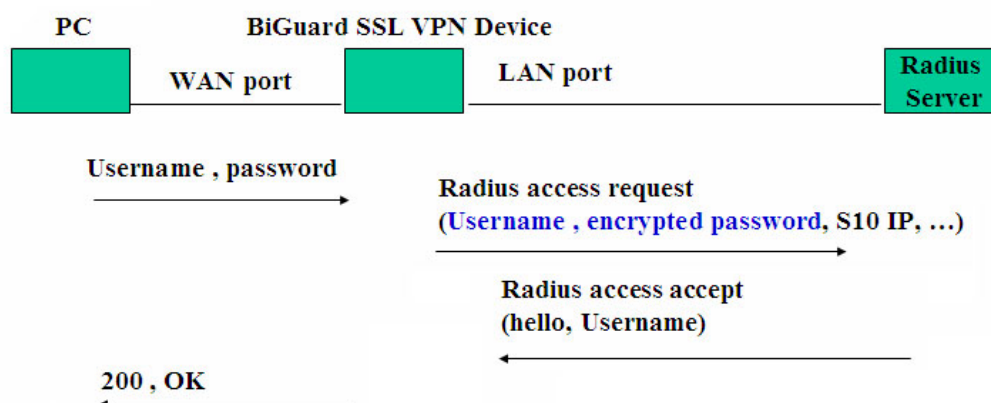


LDAP (TCP, port=389)



LDAP is based on the TCP protocol and the service port number is 389. The above diagram displays the protocol flow of LDAP.

RADIUS (UDP, port=1812)



RADIUS is based on the UDP protocol and the service port number is 1812. The above diagram displays the protocol flow of RADIUS.

Set up Example

■ Active Directory

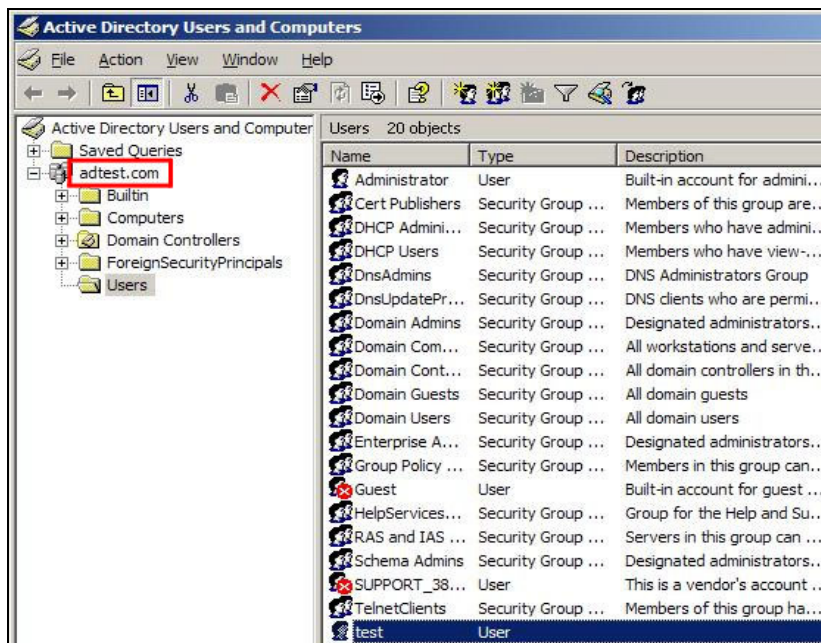
Active Directory is only available with Windows server 2000/2003, and it can be found under **Start → Program Files → Administrative Tools → Active Directory Users and Computers**. Before proceeding to step1, the Active Directory server has to be installed on your server.

Three Solutions in One



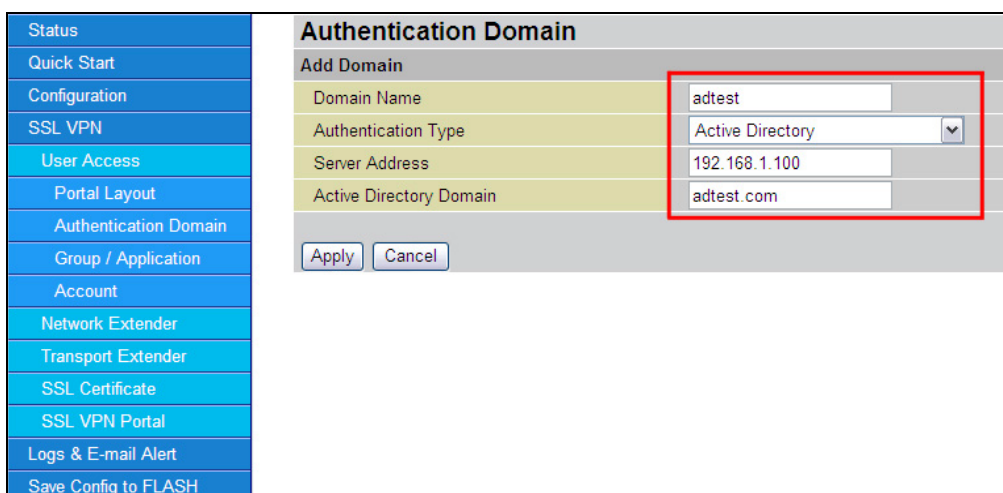
Step 1: Set up a User Account on the Active Directory server:

AD Domain Name: **adtest.com** User name: **test**



Step 2: Click **SSL VPN** → **User Access** → **Authentication Domain**.

Setup an Authentication Domain in the BiGuard SSL VPN appliances.



Domain Name: Input a name that will identify this **Active Directory Domain**.

Authentication Type: Please select **Active Directory** from the drop-down menu.

Server Address: Enter the Active Directory server IP address.

Active Directory Domain: Enter the Active Directory Domain name.

Three Solutions in One



Step 3: Click **SSL VPN** → **User Access** → **Account**

Status	<h3>Add Account</h3> <p>General Setting</p> <p>User Name: <input type="text" value="test"/></p> <p>Group: <input type="text" value="adtest"/></p> <p>Inactivity Timeout: <input type="text" value="5"/> Minutes</p> <p>Service</p> <p>Network Places: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Network Extender Service: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Transport Extender Service: <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>Web Cache Cleaner: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Network Extender IP Assignment: <input checked="" type="radio"/> Dynamic Assign <input type="radio"/> Fix IP <input type="text" value="192.168.1.240"/></p> <p>Greeting String: <input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL VPN Se"/></p> <p>Application Proxy</p> <p>Applications: This group has no application now.</p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>
Quick Start	
Configuration	
SSL VPN	
User Access	
Portal Layout	
Authentication Domain	
Group / Application	
Account	
Network Extender	
Transport Extender	
SSL Certificate	
SSL VPN Portal	
Logs & E-mail Alert	
Save Config to FLASH	

User Name: Enter a name that will identify this account in the Active Directory server.

Group: Please select **adtest** from the drop-down menu.

■ NT Domain

Step 1: Click **SSL VPN** → **User Access** → **Authentication Domain**.

Setup an Authentication Domain in the BiGuard SSL VPN appliances.

Status	<h3>Authentication Domain</h3> <p>Add Domain</p> <p>Domain Name: <input type="text" value="TestNTDomain"/></p> <p>Authentication Type: <input type="text" value="NT Domain"/></p> <p>Server Address: <input type="text" value="192.168.1.100"/></p> <p>NT Domain Name: <input type="text" value="testdomain"/></p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>
Quick Start	
Configuration	
SSL VPN	
User Access	
Portal Layout	
Authentication Domain	
Group / Application	
Account	
Network Extender	
Transport Extender	
SSL Certificate	
SSL VPN Portal	
Logs & E-mail Alert	
Save Config to FLASH	

Domain Name: Enter a name that will identify this **NT Domain**.

Authentication Type: Please select **NT Domain** from the drop-down menu.

Server Address: Enter the NT Domain server IP address.

NT Domain Name: Enter the NT Domain name.

Three Solutions in One



Step 2: Click **SSL VPN** → **User Access** → **Account**

Status	<h3>Add Account</h3> <p>General Setting</p> <p>User Name: <input type="text" value="test"/></p> <p>Group: <input type="text" value="TestNTDomain"/></p> <p>Inactivity Timeout: <input type="text" value="5"/> Minutes</p> <p>Service</p> <p>Network Places: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Network Extender Service: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Transport Extender Service: <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>Web Cache Cleaner: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Network Extender IP Assignment: <input checked="" type="radio"/> Dynamic Assign <input type="radio"/> Fix IP <input type="text" value="192.168.1.240"/></p> <p>Greeting String: <input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL VPN Se"/></p> <p>Application Proxy</p> <p>Applications: This group has no application now.</p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>
Quick Start	
Configuration	
SSL VPN	
User Access	
Portal Layout	
Authentication Domain	
Group / Application	
Account	
Network Extender	
Transport Extender	
SSL Certificate	
SSL VPN Portal	
Logs & E-mail Alert	
Save Config to FLASH	

User Name: Enter a name that will identify this account in the NT Domain server.

Group: Please select **TestNTDomain** from the drop-down menu.

■ LDAP

Step 1: Click **SSL VPN** → **User Access** → **Authentication Domain**.

Setup an Authentication Domain in the BiGuard SSL VPN appliances.

Status	<h3>Authentication Domain</h3> <p>Add Domain</p> <p>Domain Name: <input type="text" value="ldap"/></p> <p>Authentication Type: <input type="text" value="LDAP"/></p> <p>Server Address: <input type="text" value="192.168.1.100"/></p> <p>LDAP BaseDN: <input type="text" value="cn=users,dc=bgs10,dc=com"/></p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>
Quick Start	
Configuration	
SSL VPN	
User Access	
Portal Layout	
Authentication Domain	
Group / Application	
Account	
Network Extender	
Transport Extender	
SSL Certificate	
SSL VPN Portal	
Logs & E-mail Alert	
Save Config to FLASH	

Domain Name: Enter a name that will identify this **LDAP** server.

Authentication Type: Please select **LDAP** from the drop-down menu.

Server Address: Enter the LDAP server IP address.

LDAP BaseDN: Enter the LDAP BaseDN. (Example used is **cn=users, dc=bgs10, dc=com, dc=tw**)

Three Solutions in One



Step 2: Click **SSL VPN** → **User Access** → **Account**

Status	<h3>Add Account</h3> <p>General Setting</p> <p>User Name: <input type="text" value="test"/></p> <p>Group: <input type="text" value="ldap"/></p> <p>Inactivity Timeout: <input type="text" value="5"/> Minutes</p> <p>Service</p> <p>Network Places: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Network Extender Service: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Transport Extender Service: <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>Web Cache Cleaner: <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Network Extender IP Assignment: <input checked="" type="radio"/> Dynamic Assign <input type="radio"/> Fix IP <input type="text" value="192.168.1.240"/></p> <p>Greeting String: <input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text" value="Welcome to SSL/IPSEC \"/></p> <p>Application Proxy</p> <p>Applications: This group has no application now.</p> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>
Quick Start	
Configuration	
SSL VPN	
User Access	
Portal Layout	
Authentication Domain	
Group / Application	
Account	
Network Extender	
Transport Extender	
SSL Certificate	
SSL VPN Portal	
Logs & E-mail Alert	
Save Config to FLASH	

User Name: Enter a name that will identify this account in the LDAP server.

Group: Please select **ldap** from the drop-down menu.

■ RADIUS

RADIUS is available with Windows server 2000/2003 and Linux. In Windows, it can be found under **Start**→**Program Files**→**Administrative Tools**→**Internet Authentication Service**. Before setting up the RADIUS client and server, the IAS server has to be installed in your server.

RADIUS Server Settings

In the RADIUS server settings, you have to set up the RADIUS client IP address and Shared secret. In this example, client IP address is 192.168.1.254 (BiGuard S10 IP address).

The screenshot shows the 'Internet Authentication Service' console with a tree view on the left containing 'Internet Authentication Service (Local)', 'RADIUS Clients', 'Remote Access Logging', 'Remote Access Policies', and 'Connection Request Processing'. The main pane shows a table of RADIUS clients with columns for 'Friendly Name', 'Address', 'Protocol', and 'Client-Vendor'. One client named 'test' is selected, with address '192.168.1.254' and protocol 'RADIUS'. The 'test Properties' dialog box is open, showing the 'Settings' tab. The 'Friendly name' is 'test', 'Address (IP or DNS)' is '192.168.1.254', and 'Client-Vendor' is 'RADIUS Standard'. The 'Shared secret' field is empty and highlighted with a red box.

Three Solutions in One



RADIUS Router Settings

Step 1: Click **SSL VPN** → **User Access** → **Authentication Domain**.

Setup an Authentication Domain in the BiGuard SSL VPN appliances.

Status	<h3>Authentication Domain</h3> <p>Add Domain</p> <table border="1"> <tr> <td>Domain Name</td> <td><input type="text" value="radius"/></td> </tr> <tr> <td>Authentication Type</td> <td><input type="text" value="RADIUS - CHAP"/></td> </tr> <tr> <td>Server Address</td> <td><input type="text" value="192.168.1.100"/></td> </tr> <tr> <td>Secret Password</td> <td><input type="text" value="123456789"/></td> </tr> </table> <p><input type="button" value="Apply"/> <input type="button" value="Cancel"/></p>	Domain Name	<input type="text" value="radius"/>	Authentication Type	<input type="text" value="RADIUS - CHAP"/>	Server Address	<input type="text" value="192.168.1.100"/>	Secret Password	<input type="text" value="123456789"/>
Domain Name		<input type="text" value="radius"/>							
Authentication Type		<input type="text" value="RADIUS - CHAP"/>							
Server Address		<input type="text" value="192.168.1.100"/>							
Secret Password		<input type="text" value="123456789"/>							
Quick Start									
Configuration									
SSL VPN									
User Access									
Portal Layout									
Authentication Domain									
Group / Application									
Account									
Network Extender									
Transport Extender									
SSL Certificate									
SSL VPN Portal									
Logs & E-mail Alert									

Domain Name: Enter a name that will identify this **RADIUS** server.

Authentication Type: Please select **RADIUS-CHAP /RADIUS-MSCHAP/ RADIUS-PAP /RADIUS-MSCHAPV2** from the drop-down menu.

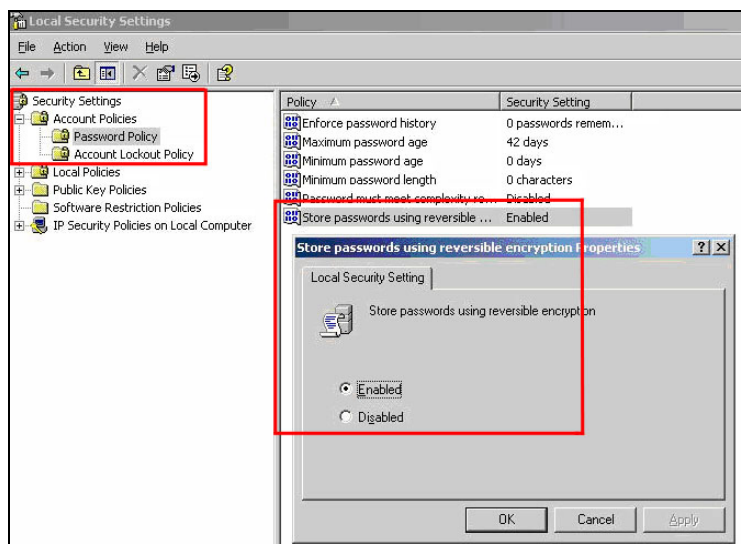
Server Address: Enter the **RADIUS** server IP address.

Secret Password: Enter the **RADIUS Shared Secret**.

NOTE: You have to enable the encryption setup in the RADIUS server in order to be compatible with RADIUS-CHAP server settings.

Click **Start**→**Program Files**→**Administrative Tools**→**Local Security Settings**

When using **RADIUS-CHAP**, please enable **Store passwords using reversible encryption** which can be found in **Password Policy**.



BiGuard

Three
Solutions
in One



© Billion Electric Co., Ltd. All rights reserved.

BiGuard user registration: www.biguard.com

Technical Support: biguardsupport@billion.com

E-mail: sales@billion.com marketing@billion.com

www.billion.com

BiGuard S10

Technical Note – Authentication Domain