

Technical Note: SecureSync

LDAP AND RADIUS AUTHENTICATION WITH A SPECTRACOM SECRESYNC

Purpose: The purpose of this document is to provide supplemental information regarding Radius and LDAP authentication in a Spectracom SecureSync.

Introduction

The Spectracom SecureSync supports LDAP and Radius authentication. Both LDAP and Radius authentication are available methods to allow the login accounts/passwords for user accounts to be stored and maintained in a central LDAP or Radius server on the network, instead of residing in the SecureSync. This function greatly simplifies password management. Instead of having to change the password in many network appliances when a password needs to be changed, if a user password is changed in the LDAP or Radius server, it automatically changes the login password for all of the appliances that are using the LDAP or Radius server to authenticate a user login.

Unlike the earlier Spectracom Model 9200 and 9300 series NTP servers, user-accounts for LDAP users do not need to be created in the SecureSync, in order for LDAP authentication to work with any access service and for Radius authentication to work with the web browser login (as discussed in the Radius section of this document, Radius authentication is limited to just the HTTP/HTTPS web browser Service. Radius authentication is not available for telnet/FTP connections or SSH/SFTP/SCP connections. These other services require local user account login via User accounts created//stored in SecureSync).

In order to use the LDAP or Radius authentication capability of the SecureSync, it needs to first be configured with the appropriate settings in order to be able to communicate with the LDAP or Radius server(s) on the network. This document expands on the information contained in the instruction manual for the SecureSync.

Refer to [Section 1](#) of this document for specific information regarding the use of **LDAP** authentication.

Refer to [Section 2](#) of this document for specific information regarding the use of **Radius** authentication.

SECTION 1: USING LDAP AUTHENTICATION

LDAP (Lightweight Directory Access Protocol) is an Internet Protocol that is used to look up information from another server. It is one of the two available methods to allow remote password authentication of a user login to the SecureSync. The SecureSync has configurations available to define the LDAP server(s) on the network and the settings in which LDAP's server should start to search its database for the applicable password.

“LDAP Server Configuration” Details

Below is some information about the LDAP server settings which are configured in SecureSync (as determined by the LDAP server).

Distinguished name of the search base (known as DN): This is the base name to use in the database search. Typically, this is the top-level of the directory tree structure. It describes where to load the users and groups.

Note: If you've customized where users are stored, you'll just need to replicate that folder structure using LDAP syntax.

Distinguished Name to bind server with (known as Bind DN): The bind DN is the user on the external LDAP server permitted to search the LDAP directory within the defined search base. Most of the time, the bind DN will be permitted to search the entire directory. The role of the bind DN is to query the directory using the LDAP query filter and search base for the DN (distinguished name) for authenticating users. When the DN is returned, the DN and password are used to authenticate the user. Enter The DN to use to bind to (this is an optional field if the database allows anonymous simple authentication). Able to use any same level of the tree and everything below.

Credential to bind server with: Either the necessary password to bind with the LDAP Server (must have read rights for all user and group data- if using Group Authentication- such as the directory administrator account password) or leave this field empty for anonymous simple authentication (by default, Active Directory does not allow anonymous LDAP connections).

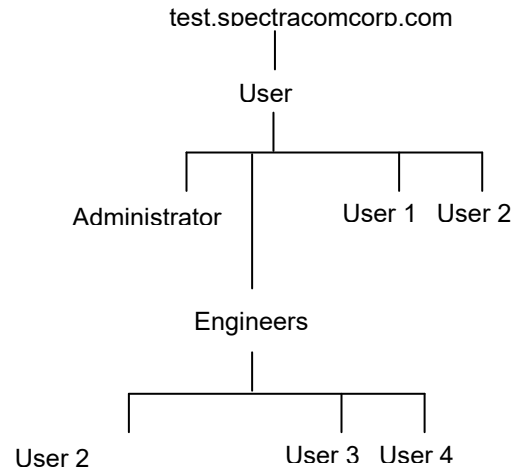
Login attribute used for search: A string of data that provides additional filter (UID) information.

Search base for password: Helps the LDAP Server determine the starting point in the directory tree to start searching for the password. Think of the search base as the "top" of the directory for your LDAP users although it may not always be the top of the directory itself. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.

Here is a sample configuration for Active Directory:

DN for search base	DC=test, DC =spectracomcorp, DC=com
Bind DN	CN=administrator,CN=users, DC=test, DC=spectracomcorp, DC=com
Bind password	test
Search filter	objectclass=User
Login attribute	sAMAccountName
DN for password	OU=users,dc=test, DC=spectracomcorp, DC=com?one
Group DN	CN=engineer,cn=users, DC=test, DC=spectracomcorp, DC=com
Group member attribute	member

The directory tree for the above example



LDAP Binding

Binding determines at which level a user has rights to. They will have rights for everything at that particular level and below but don't have rights above that value. In the above diagram, if a user is "bound" to Engineers, they can login to Engineers or Users 2-4 but not Users 1 and 2.

Notes:

- 1) All "DC=" and "CN=" in the fields should be capitalized (especially for Active Directory).
- 2) The "Login attribute..." field is case-sensitive. So if it's set to "**sAMAccountName**", it should be entered exactly as shown in the screenshot (especially for Active Directory).

LDAP Protocol versions

According to Microsoft, LDAP 3 is compatible with LDAP 2. An LDAP 2 client (such as SecureSync) can connect to an LDAP 3 server (this is a requirement of an LDAP 3 server). However, an LDAP 3 server can choose not to talk to an LDAP 2 client (such as SecureSync) if LDAP 3 features are critical to its application.

A) SecureSync LDAP Configuration (software versions 5.1.2 and above)

Configuring the Default Port and “Global” Default Gateway

If the LDAP server is not on the same subnet as the time server, the default Gateway Address needs to be properly configured in the SecureSync. As the LDAP messages are originating from within the SecureSync (they are unsolicited packets), the route for the traps to take in order to reach the configured LDAP Server(s) needs to be defined, via the Default Global Gateway. Also, if the Model 1204-06 Gigabit Ethernet Option card is installed (to add three additional Ethernet interfaces), the Ethernet interface that can route the LDAP messages to the LDAP server(s) also needs to be selected (known as the “Default Port”).

With software versions 5.1.2 or higher installed, and if the Model 1204-06 Gigabit Ethernet Option Card is installed, the Ethernet Interface to route the packets to the Internet is configured in the **Management -> Network** page of the browser, “**General Settings**” button which is located in the upper-left corner of the browser. This interface is defined in the “**Default port**” field.

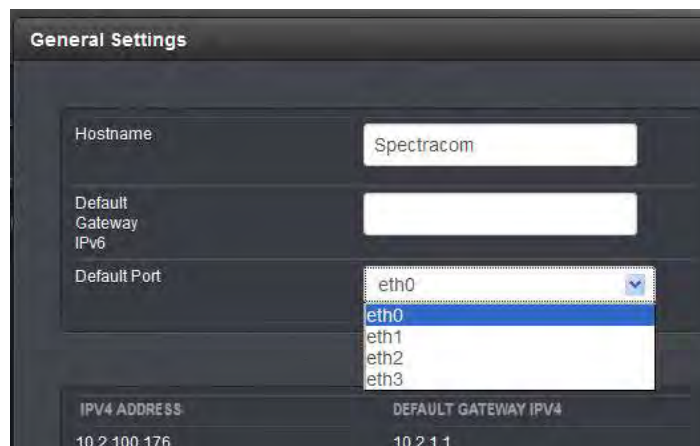
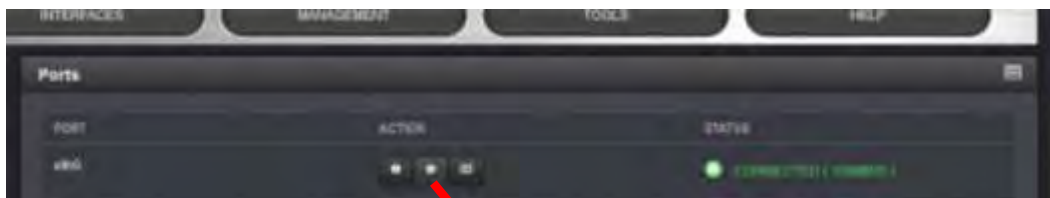


Figure 1: Configuring the Default Port (versions 5.1.2 and higher)

The default gateway address for the selected Ethernet Interface (“default port”) is configured in the “**Ports**” section of the **Management -> Network** page of the browser.

To configure the default gateway address, first press the “gear” box (center of the three boxes in the row for the Default port (such as “Eth 0” for example)). This will open a new window. If the “**Enable DHCPv4**” checkbox is not selected, the default gateway address can be defined in the “**IPv4 Gateway**” field). If the “**Enable DHCPv4**” checkbox is selected, the default gateway address should be automatically configured via the DHCP server (when this checkbox is selected, the “**IPv4 Gateway**” field won’t be displayed in this window).

Note: The same info applies if you are using an IPv6 network, except the associated fields for IPv6 networks are the “**Enable DHCPv6**” checkbox and the “**IPv6 Gateway**” field.



The screenshot shows a configuration page with the following fields and options:

- Enable DHCPv4
- Domain:
- DNS Primary:
- DNS Secondary:
- Enable DHCPv6
- Static IPv4 Address:
- Subnetmask:
- IPv4 Gateway:
- Enable DHCPv6
- Enable SLAAC
- IPv6 Gateway:

Figure 2: Configuring the default gateway (versions 5.1.2 and higher)

- Now refer to the information below for specific LDAP configuration

Process to allow access again if you are inadvertently locked out of the browser while configuring LDAP (software versions 5.3.0 and above)

If by chance you happen to lock yourself out of the web browser while configuring LDAP (due to a misconfiguration of the settings, especially when using LDAP and Radius Authentication in conjunction with each other), starting in software version 5.3.0, both LDAP and Radius can be simultaneously disabled via the front panel.

To turn off both LDAP and Radius authentication (allowing local login) use the front panel LCD/keypad **System** -> **Cmd** menu to perform a **resetpw** command. In software versions 5.3.0 and above (released ~Aug 2015), performing this front panel command will simultaneously disable both LDAP and Radius as well as also restore the spadmin account password back to the default setting of **admin123**. After regaining access to the browser again via local login, the spadmin account password can then be changed as desired and LDAP and/or Radius can be re-enabled.

Note: SecureSync software update version 5.1.2 incorporated a new web browser interface. It also incorporated a change to the LDAP functionality to allow users who can successfully login to the web browser to have administrative privileges. With earlier software versions installed, and after logging into the web browser through the LDAP servers, fields were visible, but grayed-out.

For information regarding available SecureSync software updates, please visit us at:

<http://www.spectracomcorp.com/Support/HowCanWeHelpYou/Software/tabid/61/Default.aspx#NetClock>

Please note: SecureSync requires commas (,) be used as separators between multiple values that are entered in the same field. It does not accept periods (.) as a separator between values.

1. First, navigate to the **Management** -> **Authentication** page of the browser,
2. Click the **LDAP Setup** button (left side of the page, under "Actions").
3. In the **"Servers** tab, using URI format (see the "Important Notice" below) enter the IP address or DNS name of at least one the LDAP server on the network you wish to authenticate with. Note that up to five LDAP servers on the network can be added. After entering each Server's hostname/IP address, press the **"Add Server"** button. Click

the “Servers” tab again to view the current list of LDAP servers that have been added, to add additional LDAP Servers or to remove undesired LDAP servers.

Important Notice: the LDAP server(s) **must** be entered in LDAP “URI” format (the configured value must begin with the following: **ldap://**) whether configuring the LDAP server’s hostname or IP address. Not adding **ldap://** to the beginning of every configured server’s IP address or hostname will cause ldap login to fail due to a “bad parameter”.

Example URI format include: **ldap://10.2.3.4** or **ldap://spectracom.orioia.com**

Note that in at least software versions 5.1.5 and below, the “LDAP Server Status” field will report “Configuration missing” (as shown below), though at least one LDAP server has been listed correctly.

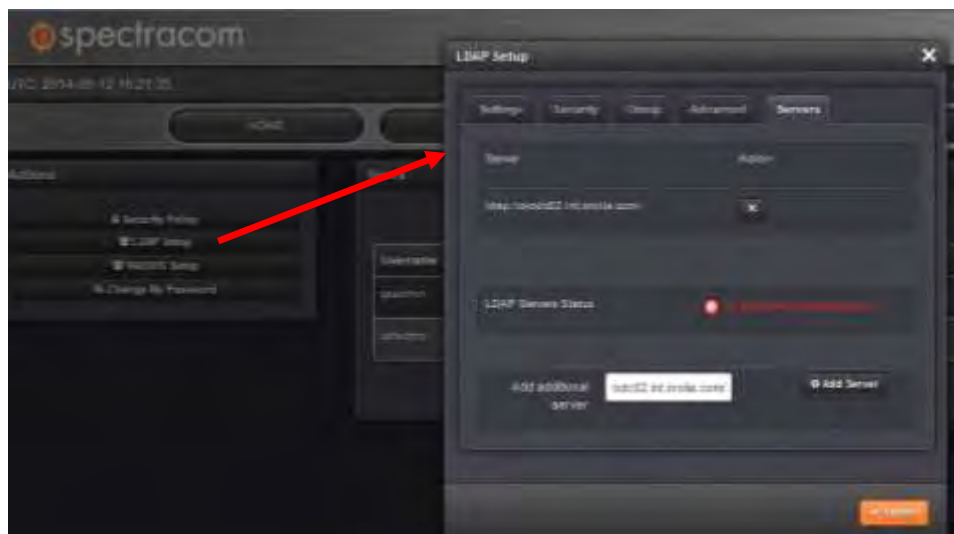
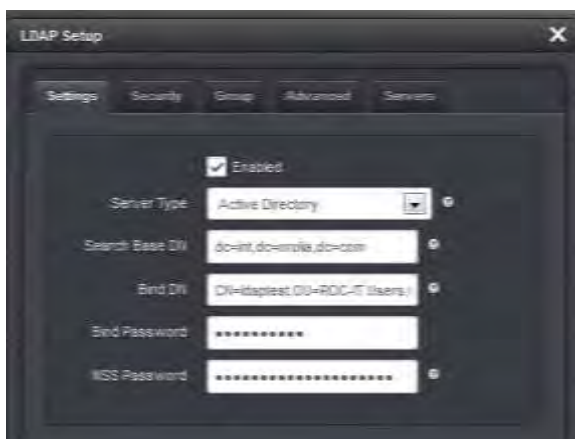
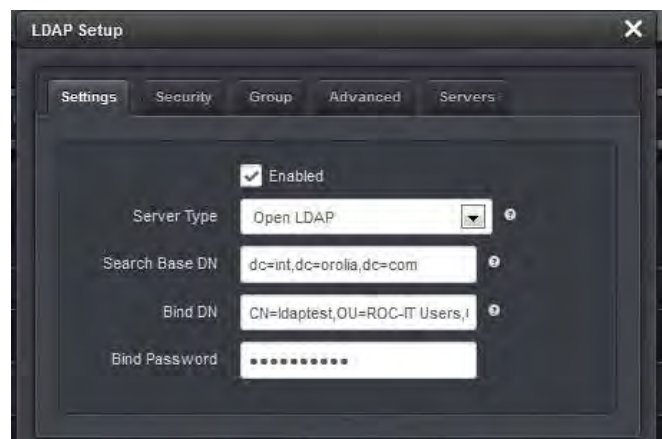


Figure 3: Servers Configuration tab of the “LDAP Setup” menu

4. Select the “Settings” tab.
 - A. Select the “Enabled” checkbox (to enable LDAP)
 - B. Select the desired LDAP “Server Type” (either “OpenLDAP” or Windows “Active Directory”)



“Server Type” set to “Active Directory”



“Server Type” set to “Open LDAP”

Figure 4: “Servers” configuration tab of the “LDAP Setup” menu

- C. Fill in all the remaining fields with information that matches your LDAP server configuration and press Submit. Note that the “NSS Password” field is only displayed when the “Server Type” field (in the “Settings” tab) is set to “Active Directory”. This field is mandatory when displayed.

NSS LDAP Access control for users

NSS password (also referred to as “NSS_base_passwd”)

Refer to sites such as: <https://www.samba.org/samba/docs/man/Samba-Guide/happy.html>, <https://help.ubuntu.com/community/ActiveDirectoryHowto> (the “libnss-ldap” section) and <http://linux.web.cern.ch/linux/docs/account-mgmt.shtml>).

The following info and an example NSS password (in red) is from:

<https://help.ubuntu.com/community/ActiveDirectoryHowto>

Modify cn=User,dc=e... to your container with your users.

```
nss_base_passwd cn=User,dc=example,dc=com?sub
nss_base_shadow cn=User,dc=example,dc=com?sub
nss_base_group cn=User,dc=example,dc=com?sub
```

The following info and an example NSS password (in red) is from:

<http://linux.web.cern.ch/linux/docs/account-mgmt.shtml>:

The NSS password (Name Service Switch) is a filter which limits the search results to all Unix accounts in Active Directory.

Syntax

nss_base_XXX base?scope?filter, where scope is {base,one,sub} and filter is a filter to be &'d with the default filter. You can omit the suffix eg: nss_base_passwd ou=People, to append the default base DN but this may incur a small performance impact.

```
nss_base_passwd OU=Users,OU=Organic Units,DC=cern,DC=ch?one
nss_base_group OU=Workgroups,DC=cern,DC=ch?sub?gidNumber=*
```


LDAP Setup

Settings Security Group Advanced Servers

Enabled

Server Type: Active Directory

Search Base DN: dc=int,dc=orolia,dc=com

Bind DN: CN=ldaptest,OU=ROC-IT Users,OU=...

Bind Password: [Redacted]

NSS Password: [Redacted]

Submit

Figure 5: “Settings” tab of the “LDAP Setup” menu (with Server Type set to Active Directory)

5. Select the “Advanced” tab. Configure the “Search Filter” and “Login Attribute” as determined by the LDAP server

LDAP Setup

Settings Security Group Advanced Servers

Search filter: objectclass=user

Login Attribute: sAMAccountName

Verify Certificate (checkpeer)

Submit

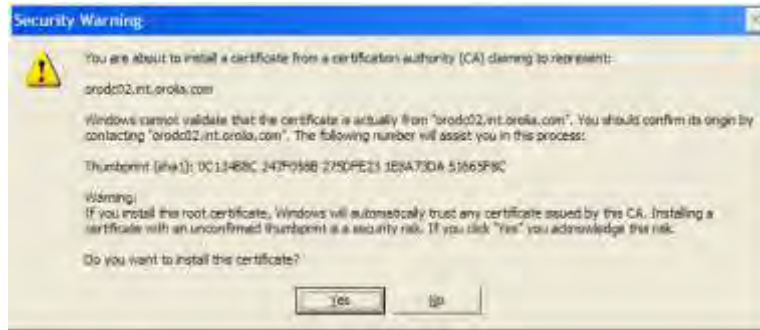
Figure 6: “Advanced” tab of the “LDAP Setup” menu

SSL Settings (optional)

Spectracom recommends enabling SSL Authentication for LDAP to encrypt passwords. Otherwise, passwords are sent over the network without encryption (“in the clear”). Enabling SSL requires obtaining the public key from the LDAP server and loading it in SecureSync.

Using Windows Certificate Manager to generate an SSL certificate

First, the LDAP’s Server key needs to be installed on the PC. If this certificate hasn’t already been installed, go to Start->Run and type `certmgr.msc`. In “Action” -> “All tasks”, select “Import”. Then browse to the location of the Server certificate and select it. Select “Automatically select the certificate store based on the type of certificate”. Select Yes to the Security Warning that is displayed.



This should install the certificate in the **Trusted Root Certification Authority/Certificates** folder. It should also generate a public certificate in the **Personal/Certificates** folder. Right click on the Certificate in the **Trusted Root Certification Authority/Certificates** folder and click on **"All Tasks" -> "Export"**.

To enable SSL authentication, use the web browser to upload the public key from the LDAP server into the SecureSync (It's stored in the SecureSync's **"/home/spectracom/xfer/cert"** directory). To upload the SSL Server certificate, in the **"Security"** tab, click on the ICON to the right of **"Server Certificate"** and then **"browse"** to the location/ filename of the certificate. After you press **"Submit"**, note that the Port field in the General Settings tab is changed to 636 (the default LDAP port for SSL access).

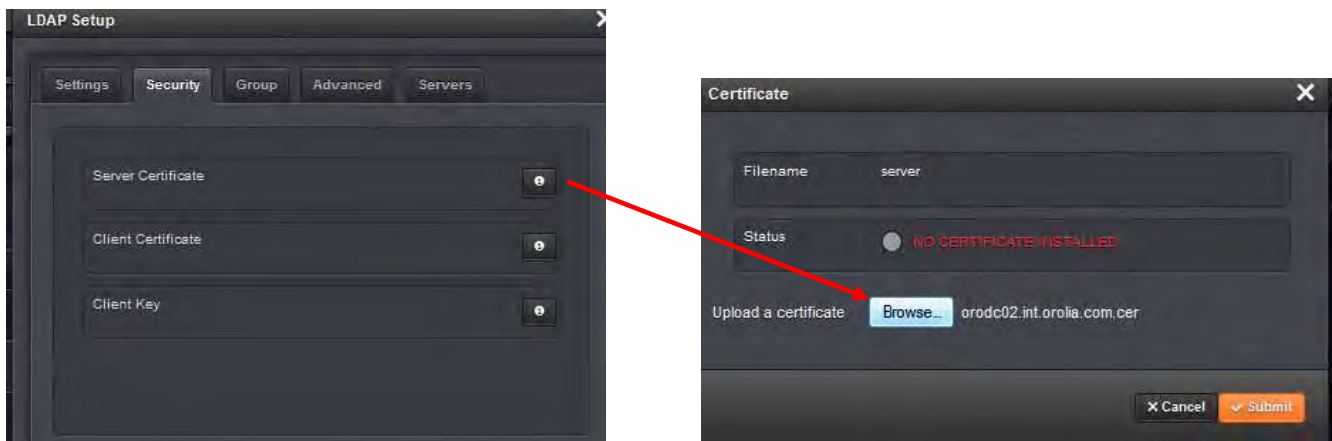


Figure 7: SSL authentication

To verify the certificate was loaded and is valid (or to upload another Server certificate) click on the ICON to the right of **"Server Certificate"** again. The Status field should report that the **"Certificate is Valid"** (in green).



Figure 8: Certificate uploaded successfully

Group-based LDAP authentication

SecureSync supports LDAP group authentication. To enable/configure group authentication, select the “Group” tab. Enable “group filter” and configure the Group settings in this tab, as required for the LDAP server.

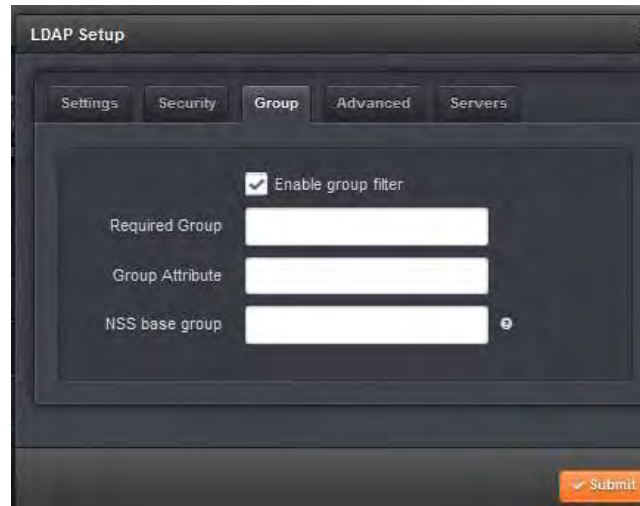


Figure 9: Group Authentication

Specific LDAP Server Configuration

Follow the instructions specific to your LDAP server(s) to create and modify users in the LDAP server(s).

A SecureSync LDAP user needs the following LDAP fields:

homeDirectory	/home/spectracom
loginShell	/bin/bash
uid	A user name, (not “spadmin”)
uidNumber	Use a number outside the range 1000 to 1050
gidNumber	“admin” group is “111”, “user” group is “112” (See the Note below)
userPassword	<password>

Note: “gidNumber” defines the permissions for each account, to be either **admin** account or **user** account. User account permissions for configuration capabilities are limited. Many of the web browser fields will be grayed-out when logged into the SecureSync’s web browser with an account using the user group.

Important Notice: Do not take a User already configured on the SecureSync and add that user to the LDAP server. In particular, do not add the “spadmin” user to the LDAP server, as this could lead to the default “spadmin” account being locked out of the web browser.

After configuring the Server and SecureSync settings, LDAP authentication can be tested. Ensure that LDAP users can log into the Web UI.

Note: Any configuration changes that are made to the SecureSync, whether via the admin account or a user account, are logged in the Journal log in the SecureSync. This log can be found on the **Tools -> Logs** page of the browser. “**Journal**” tab. The Journal log contains information on when the configuration change was made and which account made the change.

B) SecureSync LDAP Configuration (software versions 5.0.2 and below using the “classic Interface” web browser)

Note: SecureSync Archive software update version 5.1.2 incorporated a change to the LDAP functionality to allow users who can successfully login to the web browser to have administrative privileges. With earlier software versions installed, and after logging into the web browser through the LDAP servers, fields were visible, but grayed-out.

For information regarding available NetClock software updates, please visit us at:

<http://www.spectracomcorp.com/Support/HowCanWeHelpYou/Software/tabid/61/Default.aspx#NetClock>

1. First, navigate to the **Network -> LDAP Setup** web page of the browser, and then to the “LDAP Servers Configuration” tab. Enter the IP address(es) or DNS name(s) of the LDAP server(s) on the network you wish to authenticate with. Note that up to five LDAP servers on the network can be added.

LDAP Servers	Hostname / IP Address
Server 1	10.2.100.1
Server 2	
Server 3	
Server 4	
Server 5	

Figure 10: OpenLDAP LDAP Servers Configuration

2. Then, after entering at least one LDAP server, fill in the other fields below the address fields with information that matches your LDAP server configuration.

Please note: SecureSync requires commas (,) be used as separators between multiple values that are entered in the same field. It does not accept periods (.) as a separator between values.

“LDAP Servers Configuration” Details:

Below is some information about the LDAP server settings which are configured in SecureSync (as determined by the LDAP server).

Distinguished name of the search base (known as DN): This is the base name to use in the database search. Typically, this is the top-level of the directory tree structure. It describes where to load the users and groups.

Note: If you've customized where users are stored, you'll just need to replicate that folder structure using LDAP syntax.

Distinguished Name to bind server with (known as Bind DN): The bind DN is the user on the external LDAP server permitted to search the LDAP directory within the defined search base. Most of the time, the bind DN will be permitted to search the entire directory. The role of the bind DN is to query the directory using the LDAP query filter and search base for the DN (distinguished name) for authenticating users. When the DN is returned, the DN and password are used to authenticate the user. Enter The DN to use to bind to (this is an optional field if the database allows anonymous simple authentication). Able to use any same level of the tree and everything below.

Credential to bind server with: Either the necessary password to bind with the LDAP Server (must have read rights for all user and group data- if using Group Authentication- such as the directory administrator account password) or leave this field empty for anonymous simple authentication (by default, Active Directory does not allow anonymous LDAP connections).

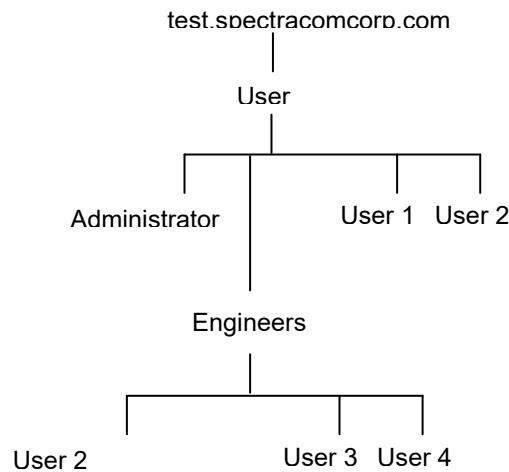
Login attribute used for search: A string of data that provides additional filter (UID) information.

Search base for password: Helps the LDAP Server determine the starting point in the directory tree to start searching for the password. Think of the search base as the "top" of the directory for your LDAP users although it may not always be the top of the directory itself. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.

Here is a sample configuration for Active Directory:

DN for search base	DC=test, DC =spectracomcorp, DC=com
Bind DN	CN=administrator,CN=users, DC=test, DC=spectracomcorp, DC=com
Bind password	test
Search filter	objectclass=User
Login attribute	sAMAccountName
DN for password	OU=users,dc=test, DC=spectracomcorp, DC=com?one
Group DN	CN=engineer,cn=users, DC=test, DC=spectracomcorp, DC=com
Group member attribute	member

The directory tree for the above example



LDAP Binding

Binding determines at which level a user has rights to. They will have rights for everything at that particular level and below but don't have rights above that value. In the above diagram, if a user is "bound" to Engineers, they can login to Engineers or Users 2-4 but not Users 1 and 2.

A sample configuration for OpenLDAP server:

DN for search base	DC=spectracomcorp,DC=com
Bind DN	CN=manager,DC=spectracomcorp,DC=com
Bind password	test
Search filter	objectclass=posixaccount
Login attribute	uid
DN for password	OU=people,DC=spectracomcorp,DC=com?one
Group DN	CN=engineer,OU=group,DC=spectracomcorp,DC=com
Group member attribute	member

Distinguished name of the search base	DC=spectracom,DC=com
Distinguished name to bind server with	spectracomcorp,DC=com
Credential to bind server with	<Password>
Search filter	objectclass=user
Login attribute used for search	sAMAccountName
Search base for password	CN=Users,?sub

Password of a user who has read access to the LDAP directory

Figure 11: Active Directory - Example - LDAP Server Configuration

Notes:

- 3) All "DC=" and "CN=" in the fields should be capitalized (especially for Active Directory).
- 4) The "Login attribute..." field is case-sensitive. So if it's set to "sAMAccountName", it should be entered exactly as shown in the screenshot (especially for Active Directory).

LDAP settings

Next, in the "General Settings" tab ("LDAP Settings" section of this page), select the LDAP Server Type (either OpenLDAP or Active Directory) and any additional LDAP settings, (the default values will work for most configurations).

LDAP SETUP

General Settings
LDAP Servers Configuration
SSL Authentication
Group Authentication

LDAP Settings

LDAP Server Type	OpenLDAP on Linux/Unix
Port for server binding	389
Time limit for searching (seconds)	120
Time limit for binding (seconds)	120
LDAP protocol version	LDAPV3
Scope to search server with	Sub

Note: There must be at least one saved LDAP server in order to configure the above settings.

Should match the setting of the LDAP server

Figure 12: General Settings**Note about LDAP Protocol version field being set to “LDAPV2”:**

According to Microsoft, LDAP 3 is compatible with LDAP 2. An LDAP 2 client (SecureSync) can connect to an LDAP 3 server (this is a requirement of an LDAP 3 server). However, an LDAP 3 server can choose not to talk to an LDAP 2 client (SecureSync) if LDAP 3 features are critical to its application.

Selecting which access services to use LDAP authentication

In the “LDAP services” section of this page, enable the access services that you wish to use the LDAP Server for authentication (such as Console/Telnet, FTP, SSH/SFTP/SCP and/or HTTP/HTTPS for the web browser).

LDAP Services	
Console Login / Telnet	Enabled
FTP	Enabled
SSH / SFTP / SCP	Enabled
HTTP / HTTPS	Enabled

Submit Reset

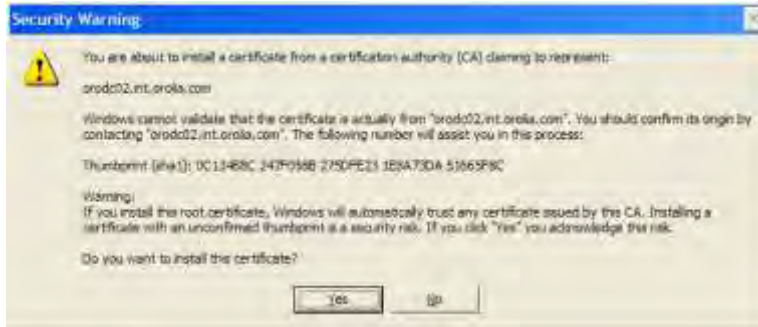
Figure 13: LDAP Services

SSL Settings

Spectracom recommends enabling SSL Authentication for LDAP to encrypt passwords. Otherwise, passwords are sent over the network without encryption (“in the clear”). Enabling SSL requires obtaining the public key from the LDAP server and loading it in SecureSync.

Using Windows Certificate Manager to generate an SSL certificate

First, the LDAP’s Server key needs to be installed on the PC. If this certificate hasn’t already been installed, go to Start->Run and type **certmgr.msc**. In “**Action**” -> “**All tasks**”, select “**Import**”. Then browse to the location of the Server certificate and select it. Select “Automatically select the certificate store based on the type of certificate”. Select Yes to the Security Warning that is displayed.



This should install the certificate in the **Trusted Root Certification Authority/Certificates** folder. It should also generate a public certificate in the **Personal/Certificates** folder. Right click on the Certificate in the **Trusted Root Certification Authority/Certificates** folder and click on “**All Tasks**” -> “**Export**”.

To enable SSL authentication, use either FTP or SCP to copy the public key from the LDAP server to the “**/home/spectracom/xfer/cert**” directory on SecureSync. Then, on the “SSL Authentication” tab, enable SSL and enter the filename of the certificate in the “CA server certificate” field. After you press “Submit”, note that the Port field in the General Settings tab is changed to 636 (the default LDAP port for SSL access).

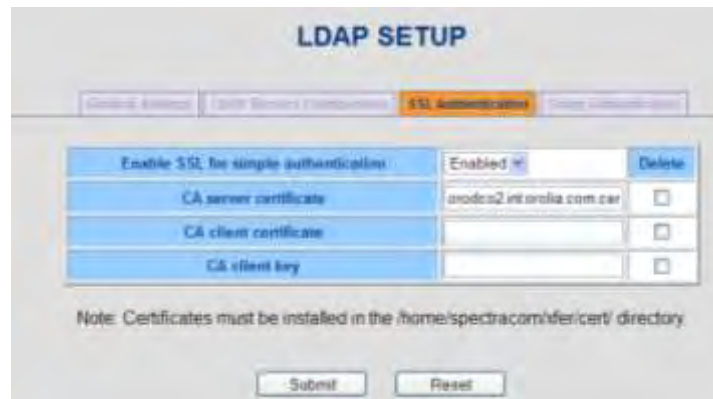


Figure 14: SSL authentication

Group-based LDAP authentication

SecureSync supports LDAP group authentication. To enable/configure group authentication, select the “Group Authentication” tab. Enable “group based authentication” and configure the Group settings in this tab.

LDAP SETUP

General Settings
LDAP Servers Configuration
SSL Authentication
Group Authentication

Enable group based authentication	<input type="text" value="Disable"/>
Group to enforce membership of	<input type="text"/>
Group member attribute	<input type="text"/>

Figure 15: Group Authentication

Specific LDAP server configuration information

Follow the instructions specific to your LDAP server(s) to create and modify users in the LDAP server(s).

A SecureSync LDAP user needs the following LDAP fields:

homeDirectory	/home/spectracom
loginShell	/bin/bash
uid	A user name, (not "spadmin")
uidNumber	Use a number outside the range 1000 to 1050
gidNumber	"admin" group is "111", "user" group is "112" (See the Note below)
userPassword	<password>

Note: "gidNumber" defines the permissions for each account, to be either **admin** account or **user** account. User account permissions for configuration capabilities are limited. Many of the web browser fields will be grayed-out when logged into the SecureSync's web browser with an account using the user group.

Important Notice: Do not take a User already configured on the SecureSync and add that user to the LDAP server. In particular, do not add the "spadmin" user to the LDAP server, as this could lead to the default "spadmin" account being locked out of the web browser.

After configuring the Server and SecureSync settings, LDAP authentication can be tested. Ensure that LDAP users can log into the Web UI.

Note: Any configuration changes that are made to the SecureSync, whether via the admin account or a user account, are logged in the Journal log in the SecureSync. This log can be found on the **Tools -> Logs** page of the browser. "Journal" tab. The Journal log contains information on when the configuration change was made and which account made the change.

LDAP Authentication process (order of precedence) / Auth log entries

When logging into the NTP server, the order of precedence is local login first. This is then followed by LDAP authentication, if the local login fails.

Logging in with HTTP/HTTPS (web browser login)

If the user account name exists in the NTP server and the login password is valid, connection to the web browser is granted/established. Successful web browser (HTTP/HTTPS) connections are not logged in the NTP server. In this situation, the LDAP server is not contacted.

However, if the user account name does not exist in the NTP server, or if the login password is not valid, the Radius server is then contacted for authentication attempt. A log entry will be asserted in the NTP Server's Authentication (Auth) log to indicate either the user account does not exist or the password entered was not valid.

Example Auth log entries in the NTP server

Example of a failed local login due to valid username (in this particular example, "spadmin") but invalid password:

```
Oct 23 14:19:25 Spectracom httpd(pam_unix)[11894]: authentication failure; logname= uid=1111 euid=1111
tty= ruser= rhost= user=spadmin
```

Example of a failed local login due to invalid username (in this particular example, the username entered was "admin1111", but there is no user account in the NTP server with this name, password entered was just arbitrary characters):

```
Oct 23 14:22:34 Spectracom pam_tally[11581]: pam_tally: pam_get_uid; no such user
```

```
Oct 23 14:22:34 Spectracom httpd(pam_unix)[11581]: authentication failure; logname= uid=1111 euid=1111
tty= ruser= rhost=
```

```
Oct 23 14:22:34 Spectracom httpd(pam_unix)[11581]: check pass; user unknown
```

If local login fails due to there being no user account in the NTP server or due to an invalid password, but the Radius server successfully authenticates the login, access is granted to the web browser. No other log entries are asserted in the NTP server for this successful login. If the Radius authentication also fails, access to the web browser is not granted and no other log entries are asserted in the NTP server.

Logging in with telnet/SSH

If the user account name exists in the NTP server and the login password is valid, connection to the web browser is granted/established. Successful telnet/SSH connections are logged in the NTP server's Authentication (Auth) log. In this situation, the LDAP server is not contacted.

However, if the user account name does not exist in the NTP server, or if the login password is not valid, the LDAP server is then contacted for an authentication attempt. A log entry will be asserted in the NTP Server's Authentication (Auth) log to indicate either the user account does not exist or the password entered was not valid.

Example Auth log entries in the NTP server

Example of a successful connection to a user account in the NTP server (in this particular example, the username is "kwing")

Oct 23 16:02:07 Spectracom sshd[32499]: error: open /dev/tty failed - could not set controlling tty: **Permission denied**

Oct 23 16:02:07 Spectracom sshd(pam_unix)[32278]: **session opened for user kwing** by (uid=0)

Example of a failed local login due to valid username (in this example, "spadmin") but invalid password:

Oct 23 13:55:41 Spectracom sshd[12306]: **error: PAM: Authentication failure for spadmin** from pm-wing2.int.oria.com

Oct 23 13:55:39 Spectracom sshd(pam_unix)[12512]: **authentication failure**; logname= uid=0 euid=0 tty=ssh ruser= rhost=pm-wing2.int.oria.com user=spadmin

Example of a failed local login due to invalid username (in this particular example, the username entered was "admin1111", but there is no user account in the NTP server with this name, password entered was just arbitrary characters)

Oct 23 14:07:10 Spectracom sshd[27122]: Postponed keyboard-interactive for invalid user admin from 10.2.100.29 port 1280 ssh2 [preauth]

Oct 23 14:07:10 Spectracom sshd[27122]: Failed keyboard-interactive/pam for invalid user admin from 10.2.100.29 port 1280 ssh2

Oct 23 14:07:10 Spectracom sshd[27122]: error: PAM: User not known to the underlying authentication module for illegal user admin from pm-wing2.int.oria.com

If local login fails due to no user account in the NTP server or due to an invalid password, but the LDAP server successfully authenticates the login, access is granted to the telnet/SSH session. No other log entries are asserted in the NTP server for this successful login. If the Radius authentication also fails, access to the telnet/SSH session is not granted and no other log entries are asserted in the NTP server.

SECTION 2: USING RADIUS PASSWORD AUTHENTICATION

Radius (Remote Authentication Dial in User Service) is a networking protocol that provides centralized Authentication, Authorization and Accounting management for computers to connect and use a network service. It is one of the available methods to allow remote password authentication of a user login to the SecureSync. The SecureSync has configurations available to define the Radius server(s) on the network and the settings in which for it to communicate with the Radius server.

The SecureSync uses PAM Radius (Pluggable Authentication Module) functionality included with the RADIUS PAM module (pam_radius_auth) from the freeradius organization. For more information on the Radius PAM module, please visit: http://freeradius.org/pam_radius_auth/.

The Radius functionality in the time server supports PAP (Password Authentication Protocol). PAP is a commonly supported authentication protocol. With PAP, the SecureSync sends the user-name and user-password to the Radius server as an Access-Request packet (which is encrypted using the configured “secret key” shared by the time server and the Radius server). The Radius server then decrypts this received packet, verifies the user using the user-password (the Radius server searches a database of users) and then informs the time server to allow access once the password has been authenticated.

Notes:

- 1) The SecureSync does not support CHAP authentication (Challenge Handshake Authentication Protocol) which provides for a triple handshake of the communications between the Radius server and the NTP server for authentication.
- 2) Do not take a user already configured on the SecureSync and add that same user to the Radius server. In particular, do not add the “spadmin” user to the Radius server as this could lead to spadmin being locked out of the web UI.
- 3) SecureSync’s Radius authentication login capability is limited to just the web browser service (HTTP/HTTPS only). Login to other non-web browser services (such as telnet/SSH, FTP/SCP, etc) is limited to local login only, using accounts/passwords that are created and stored in SecureSync.

If it’s desired for Users (accounts other than the spadmin account) to be able to login to any of these non-web browser services (such as telnet, for instance) refer to the SecureSync user manual for information on creating new User accounts.

Admin/User rights for Radius users

- All users who login to the SecureSync through Radius are automatically assigned Admin rights.
- Radius accounts can’t be assigned user rights, unless either Radius authentication is combined with LDAP Authentication as well, or a local user account is created in the SecureSync.

RADIUS only provides authentication. You provide it a username and a password, and it provides back whether that username and password is authenticated. It doesn’t provide any permissions or other authorization information. The only alternatives to allow accounts to have user rights (instead of admin rights) are to either:

- Combine RADIUS with another system that provides authorization (such as LDAP),
- Or to make local user accounts matching those that are being authenticated.

If there is a local account with the same username, it will be authenticated using RADIUS, and use the permissions from the local account.

RSA authentication

RSA authentication (SecurID) should be compatible with SecureSync. However, if you notice any problems while using RSA authentication, please let us know.

Vendor Specific Attributes (“VSA”) and Vendor ID (Vendor code)

Some network devices have Vendor Specific Attributes which are unique Radius features beyond the standard RFC specifications for Radius. VSA’s allow the vendors of these devices to support their own proprietary Radius attributes. These vendors can be assigned a vendor ID/Vendor code to be included in a dictionary.

The SecureSync does not have a vendor ID/Vendor code assigned, nor does it have any Vendor Specific Attributes (VSAs).

TACACS and iPass

Radius Authentication in conjunction with TACACS and iPass is not supported. TACACS is another type of authentication protocol that is not similar to Radius. iPass requires specialized software from the iPass organization be installed, which is not possible with the SecureSync.

- For more information on the use of Radius with a Cisco Radius server, please refer to <http://wiki.freeradius.org/Cisco>.
- For more information on Radius in general, please refer to <http://www.ietf.org/rfc/rfc2865.txt> for the Radius specs (RFC 2865).

A) SecureSync Radius Configuration (Software versions 5.1.2 and above)

Process to allow access again if you are inadvertently locked out of the web browser while configuring Radius (software versions 5.3.0 and above)

If by chance you happen to lock yourself out of the web browser while configuring Radius (due to a misconfiguration of the settings, especially when using LDAP and Radius Authentication in conjunction with each other), starting in software version 5.3.0, both LDAP and Radius can be simultaneously disabled via the front panel.

To turn off both LDAP and Radius authentication (allowing local login) use the front panel LCD/keypad System -> Cmd menu to perform a resetpw command. In software versions 5.3.0 and above (released ~Aug 2015), performing this front panel command will simultaneously disable both LDAP and Radius as well as also restore the spadmin account password back to the default setting of admin123. After regaining access to the browser again via local login, the spadmin account password can then be changed as desired and LDAP and/or Radius can be re-enabled.

Configuring the Default Port and “Global” Default Gateway

If the Radius server is not on the same subnet as the time server, the default Gateway Address needs to be properly configured in the SecureSync. As the Radius messages are originating from within the SecureSync (they are unsolicited packets), the route for the traps to take in order to reach the configured Radius Server(s) needs to be defined, via the Default Global Gateway. Also, if the Model 1204-06 Gigabit Ethernet Option card is installed (to add three additional Ethernet interfaces), the Ethernet interface that can route the Radius messages to the RADIUS server(s) also needs to be selected (known as the “Default Port”).

With software versions 5.1.2 or higher installed, and if the Model 1204-06 Gigabit Ethernet Option Card is installed, the Ethernet Interface to route the packets to the Internet is configured in the **Management -> Network** page of the browser, “**General Settings**” button which is located in the upper-left corner of the browser. This interface is defined in the “**Default port**” field.

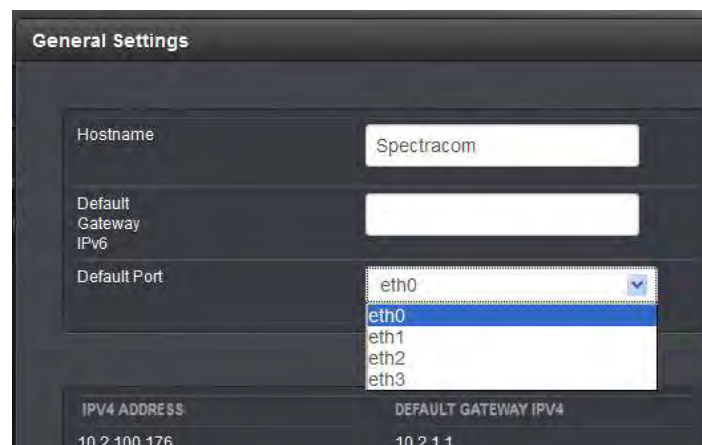


Figure 16: Configuring the Default Port (versions 5.1.2 and higher)

The default gateway address for the selected Ethernet Interface (“default port”) is configured in the “**Ports**” section of the **Management -> Network** page of the browser.

To configure the default gateway address, first press the “gear” box (center of the three boxes in the row for the Default port (such as “Eth 0” for example). This will open a new window. If the “**Enable DHCPv4**” checkbox is not selected, the default gateway address can be defined in the “**IPv4 Gateway**” field). If the “**Enable DHCPv4**” checkbox is selected, the default gateway address should be automatically configured via the DHCP server (when this checkbox is selected, the “**IPv4 Gateway**” field won’t be displayed in this window.

Note: The same info applies if you are using an IPv6 network, except the associated fields for IPv6 networks are the “**Enable DHCPv6**” checkbox and the “**IPv6 Gateway**” field.

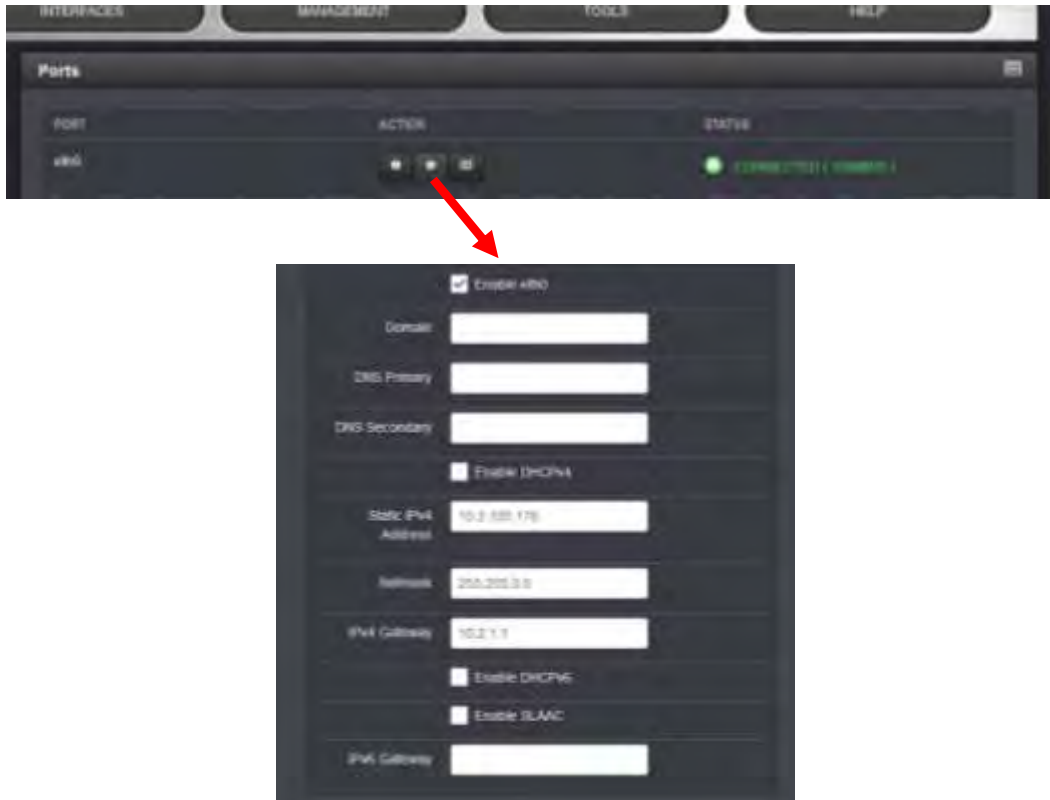


Figure 17: Configuring the default gateway (versions 5.1.2 and higher)

- Now refer to the information below for specific Radius configuration

Note: SecureSync Archive software update version 5.1.2 incorporated a new web browser interface. It also incorporated a change to the Radius functionality to allow users who can successfully login to the web browser to have administrative privileges. With earlier software versions installed, and after logging into the web browser through the Radius servers, fields were visible, but grayed-out.

For information regarding available NetClock software updates, please visit us at:

<http://www.spectracomcorp.com/Support/HowCanWeHelpYou/Software/tabid/61/Default.aspx#NetClock>

Please note: SecureSync requires commas (,) be used as separators between multiple values that are entered in the same field. It does not accept periods (.) as a separator between values.

Steps to add/configure a Radius server in the SecureSync (versions 5.1.2 and above)

1. First, navigate to the **Management -> Authentication** page of the browser, and then press the “**RADIUS Setup**” button (left side of the page, under “Actions”).

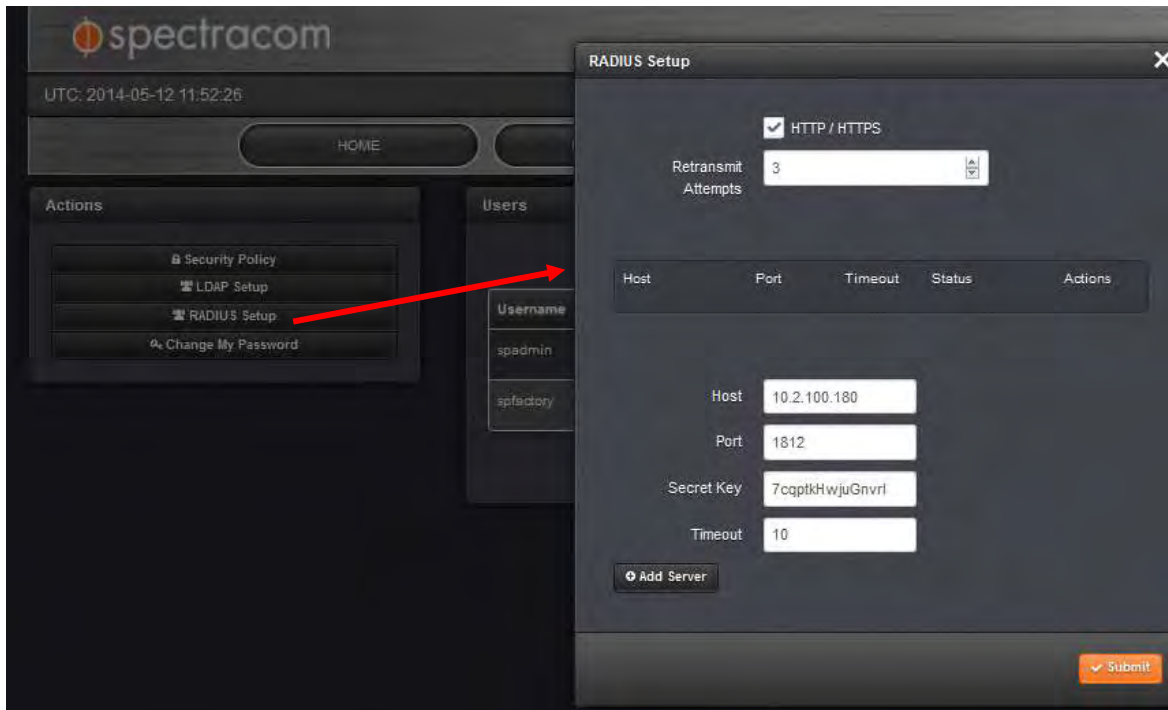


Figure 18: Radius Server Configuration

2. Select the HTTP/HTTPS checkbox at the top of the page and then press Submit to enable Radius authentication.
 3. Press the **"RADIUS Setup"** button again to re-open the Radius Setup Menu. Enter the number of desired "retransmit Attempts" (such as "3" for example).
 4. Enter the IP address(es) or DNS name(s) of each Radius server on the network you wish to authenticate with. Note that up to five Radius servers on the network can be added. If there is more than one, repeat this procedure for each server, after pressing the "Add Server" button at the bottom of this configuration menu.
 5. Enter the network port for the SecureSync to communicate with the Radius server.
 6. Enter the shared Secret key from the particular Radius server, as configured in the Radius server (The secret key generates an MD5 hash). The port number to use for communication with the Radius server and the timeout for this connection can be changed from the default values as necessary.
- Note:** Entering just the IP address/hostname of the Radius server without entering the required "Secret Key" value will result in a validation error when the Submit button is pressed. The Secret Key value needs to be entered in order for the MD5 hash to be able to be generated.
7. Enter the desired "Timeout" period, in seconds, for the SecureSync to reach this Radius sever (10 seconds, for example).
 8. Press the **"Add Server"** button to accept the settings. Repeat this procedure for each Radius Server on the network you wish to add to the SecureSync.
 9. After configuring all desired Radius Servers,
 10. The "Radius Setup" will now show the configured Radius server(s)

The “**Status**” field in the row with the configured Radius server will report whether Radius is currently enabled and if the SecureSync can successfully reach that particular Radius server, as described below:

A. REACHABLE (in green)

“**REACHABLE**” indicates the **HTTP/HTTPS** checkbox at the top of the Radius Setup menu is currently selected (Radius is enabled) and the SecureSync can successfully reach the Radius Server. Note that “Reachable” does not show that the Secret Key has been entered correctly. It just shows it can see that the Radius server is on the network with the SecureSync. The Secret Key is verified by successfully logging in to the web browser using a Radius account.

Host	Port	Timeout	Status	Actions
10.2.100.92	1812	10	● REACHABLE	<input type="button" value="X"/>

Figure 19: Status reports REACHABLE

B. DISABLED (in orange)

“**Disabled**” indicates the **HTTP/HTTPS** checkbox at the top of the Radius Setup menu isn’t currently selected. Press the “Radius Setup” button the left side of the page and select the **HTTPS/HTTPS** checkbox at the top of the “Radius Setup” menu. Then press Submit.

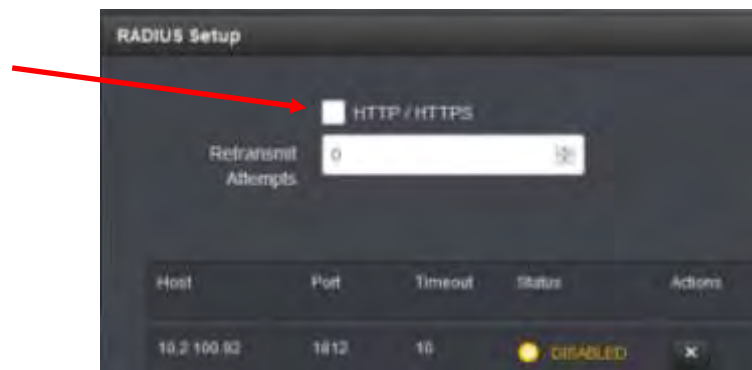


Figure 20: HTTP/HTTPS checkbox not selected

C. UNREACHABLE (in red)

“**UNREACHABLE**” indicates a Radius server that the SecureSync is not able to communicate with (the Radius server is not responding to a ping). The Host address may not be correct or the Radius server may not be on the same network as the SecureSync.

Host	Port	Timeout	Status	Actions
10.2.100.180	1812	10	● UNREACHABLE	<input type="button" value="X"/>

Figure 21: Radius Server unreachable

Potential causes for “Unreachable” to be reported

- The Radius server may just have ping disabled
- The configured Host address may not be correct
- The Radius server may not be on the same network as the NetClock (network routing issues)
- The main default port/gateway may not be configured correctly

After configuring the Radius Server and SecureSync settings, Radius authentication can be tested. Ensure that Radius users can log into the Web UI.

Note: Any configuration changes that are made to the SecureSync, whether via the admin account or a user account, are logged in the Journal log in the SecureSync. This log can be found on the **Tools -> Logs** page of the browser, “**Journal**” tab. The Journal log contains information on when the configuration change was made and which account made the change.

B) SecureSync Radius Configuration (Software versions 5.0.2 and below using the “Classic Interface” web browser)

Steps to add/configure a Radius server in the SecureSync (versions 5.0.2 and below)

Note: SecureSync Archive software update version 5.1.2 incorporated a change to the Radius functionality to allow users who can successfully login to the web browser to have administrative privileges. With earlier software versions installed, and after I **Configuring the Default Port and “Global” Default Gateway**

If the LDAP server is not on the same subnet as the time server, the default Gateway Address needs to be properly configured in the SecureSync. As the LDAP messages are originating from within the SecureSync (they are unsolicited packets), the route for the traps to take in order to reach the configured Radius Server(s) needs to be defined, via the Default Global Gateway. Also, if the Model 1204-06 Gigabit Ethernet Option card is installed (to add three additional Ethernet interfaces), the Ethernet interface that can route the Radius messages to the LDAP server(s) also needs to be selected (known as the “Default Port”).

With software versions 5.1.2 or higher installed, and if the Model 1204-06 Gigabit Ethernet Option Card is installed, the Ethernet Interface to route the packets to the Internet is configured in the **Management -> Network** page of the browser, **“General Settings”** button which is located in the upper-left corner of the browser. This interface is defined in the **“Default port”** field.

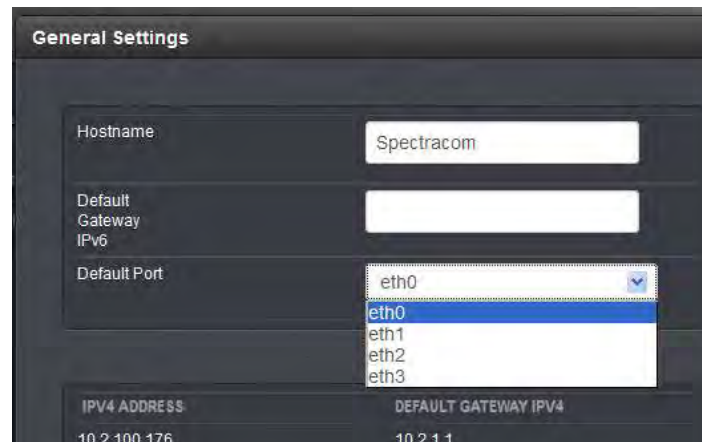
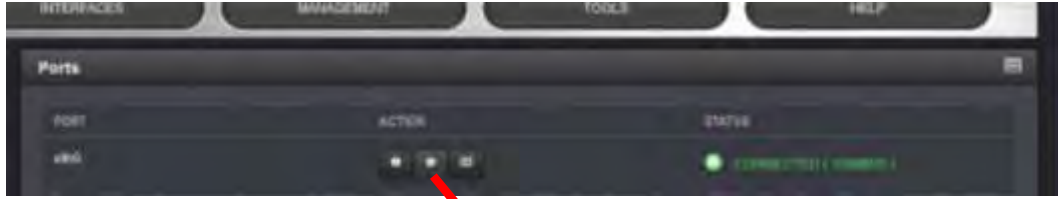


Figure 22: Configuring the Default Port (versions 5.1.2 and higher)

The default gateway address for the selected Ethernet Interface (“default port”) is configured in the **“Ports”** section of the **Management -> Network** page of the browser.

To configure the default gateway address, first press the “gear” box (center of the three boxes in the row for the Default port (such as “Eth 0” for example)). This will open a new window. If the **“Enable DHCPv4”** checkbox is not selected, the default gateway address can be defined in the **“IPv4 Gateway”** field). If the **“Enable DHCPv4”** checkbox is selected, the default gateway address should be automatically configured via the DHCP server (when this checkbox is selected, the **“IPv4 Gateway”** field won’t be displayed in this window).

Note: The same info applies if you are using an IPv6 network, except the associated fields for IPv6 networks are the **“Enable DHCPv6”** checkbox and the **“IPv6 Gateway”** field.



Enable AHO
 Domain:
 DNS Primary:
 DNS Secondary:
 Enable DHCPv4
 Static IPv4 Address:
 Subnet:
 IPv4 Gateway:
 Enable DHCPv6
 Enable SLAAC
 IPv6 Gateway:

Figure 23: Configuring the default gateway (versions 5.1.2 and higher)

- Now refer to the information below for specific Radius configuration

Logging into the web browser through the Radius servers, fields were visible, but grayed-out.

For information regarding available NetClock software updates, please visit us at:

<http://www.spectracomcorp.com/Support/HowCanWeHelpYou/Software/tabid/61/Default.aspx#NetClock>

- 1) Navigate to the Server Configuration tab of the SecureSync Network -> Radius Setup web page, “Server Configuration” tab. Enter either the IP address(es) or the Host name(s) of the desired Radius server(s) on the network to authenticate with. The SecureSync supports up to five Radius servers to be configured.

Also, enter the shared Secret key from the particular Radius server, as configured in the Radius server (The secret key generates an MD5 hash). The port number to use for communication with the Radius server and the timeout for this connection can be changed from the default values as necessary.

Note: Entering just the IP address/hostname of the Radius server without entering the required “Secret Key” value will result in a validation error when the Submit button is pressed. The Secret Key value needs to be entered in order for the MD5 hash to be able to be generated.

RADIUS SETUP

General Settings Server Configuration

	Hostname / IP Address	Secret Key	Port	Timeout (s)
Server 1	<input type="text" value="10.10.128.40"/>	<input type="text" value="<SecretKey>"/>	<input type="text" value="1812"/>	<input type="text" value="10"/>
Server 2	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="10"/>
Server 3	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="10"/>
Server 4	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="10"/>
Server 5	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="10"/>

Retransmit Attempts (1 to 5)

Submit Reset

Figure 24: Radius Server Configuration

- Only the “HTTP/HTTPS” access Service supports authentication by a Radius Server. The HTTP/HTTPS Service is enabled in the “General Settings” tab.

Note: Earlier versions of SecureSync software (versions 4.8.0 and below) display Enable/Disable fields for the other access Services, but these other listed Services cannot use Radius authentication and should always be set to “Disabled” (if these other fields are displayed in your SecureSync). Versions beyond version 4.8.0 no longer display the three other enable/disable fields.

RADIUS SETUP

General Settings Server Configuration

RADIUS Services

HTTP / HTTPS

Submit Reset

Figure 25: Radius General Settings (Archive versions 4.8.0 and higher)

Note: Do not take a user already configured on the SecureSync and add that same user to the Radius server. In particular, do not add the “spadmin” user to the Radius server as this could lead to spadmin being locked out of the web UI.

After configuring the Server and SecureSync settings, Radius authentication can be tested. Ensure that Radius users can log into the Web UI.

Note: Any configuration changes that are made to the SecureSync, whether via the admin account or a user account, are logged in the Journal log in the SecureSync. This log can be found on the **Tools** -> **Logs** page of the browser. "Journal" tab. The Journal log contains information on when the configuration change was made and which account made the change.

Radius Authentication process (order of precedence) / Auth log entries (all software versions)

When logging into the web browser, the order of precedence is local login first. This is then followed by Radius authentication, if the local login fails.

If the user account name exists in the NTP server and the login password is valid, connection to the web browser is granted/established. Successful web browser (HTTP/HTTPS) connections are not logged in the NTP server's Authentication (Auth) log. In this situation, the Radius server is not contacted.

However, if the user account name does not exist in the NTP server, or if the login password is not valid, the Radius server is then contacted for authentication attempt. A log entry will be asserted in the NTP Server's Authentication (Auth) log to indicate either the user account does not exist or the password entered was not valid.

Example auth log entries in the NTP server

Example of a failed local login due to valid username (in this example, "spadmin") but invalid password:

```
Oct 23 14:19:25 Spectracom httpd(pam_unix)[11894]: authentication failure; logname= uid=1111 euid=1111 tty=
ruser= rhost= user=spadmin
```

Example of a failed local login due to invalid username (in this particular example, the username entered was "admin1111", but there is no user account in the NTP server with this name, password entered was just arbitrary characters):

```
Oct 23 14:22:34 Spectracom pam_tally[11581]: pam_tally: pam_get_uid; no such user
```

```
Oct 23 14:22:34 Spectracom httpd(pam_unix)[11581]: authentication failure; logname= uid=1111 euid=1111
tty= ruser= rhost=
```

```
Oct 23 14:22:34 Spectracom httpd(pam_unix)[11581]: check pass; user unknown
```

If local login fails due to no user account in the NTP server or due to an invalid password, but the Radius server successfully authenticates the login, access is granted to the web browser. No other log entries are asserted in the NTP server's authentication (Auth) log for this successful login. If the Radius authentication also fails, access to the web browser is not granted and no other log entries are asserted in the NTP server.

SPECTRACOM TECHNICAL SUPPORT

Please contact one of the global Spectracom Technical Support centers for assistance:

USA www.spectracomcorp.com | techsupport@spectracomcorp.com |
1565 Jefferson Rd. | Rochester, NY 14623 | +1.585.321.5800

FRANCE www.spectracom.fr | techsupport@spectracom.fr |
3 Avenue du Canada | 91974 Les Ulis, Cedex | +33 (0)1 64 53 39 80

UK www.spectracom.co.uk | techsupport@spectracom.co.uk |
6A Beechwood | Chineham Park | Basingstoke, Hampshire, RG24 8WA |
44 (0)1256 303630