

LUNA SDAC Connectivity Guide

***** 5ghz WI-FI is not supported *****

For network connections, it is imperative to know the wireless security information from the router. Guessing can cause connections issues and frustration. Please contact router manufacturer if needed.

The following document will step through AD-HOC (peer to peer) connectivity from a WI-FI enabled PC to an SDAC, and how to then connect the SDAC to a local area network.

If the local network connection fails or changes, the AD-HOC (peer to peer) connection is always available, unless it is disabled; therefore, it is not recommended to disable the AD-HOC (peer to peer) connection.

When doing the AD-HOC (peer to peer) connection, the PCs wireless adapter does not need to be set with a static IP address. The SDAC will assign an IP address to the PC upon connection via DHCP.

When adding an SDAC to a wireless network, it is imperative to set a static IP address to the SDAC. Without a static IP address, the LUNA software will not be able to find the SDAC on the network. DHCP Reservation on the router can be done; however, it is recommended to set a static IP address within the SDAC unit.

Index:

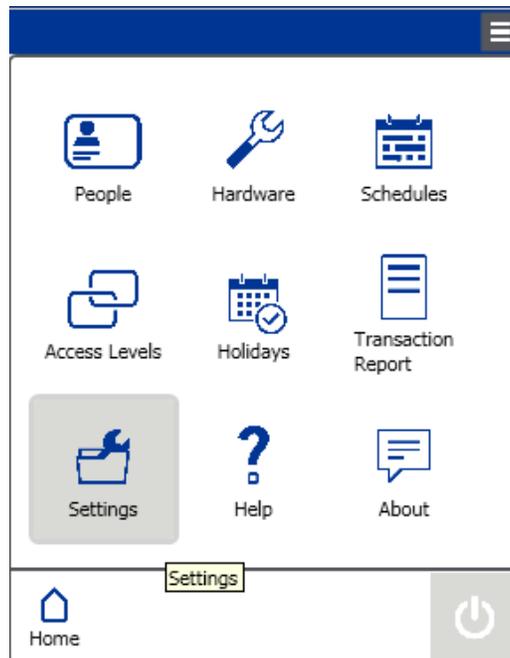
Page 1	LUNA SDAC Connectivity Guide
Page 2	Creating an Encryption Key
Page 3	AD-HOC (Peer to Peer) Connectivity
Page 5	Configuring an SDAC to Connect to a Wireless Network
Page 9	Subnets

NOTE: *This is not an official document and is not a LUNA guide or help file. This is a support guide only.*

Creating an Encryption Key

Existing installations where a new SDAC is being added, can skip encryption key setup.

For all new installations, install and launch the Luna software, then go to the *Settings* menu.



Here you will find *Communication Settings* and a field called *Encryption Key*. This a 64bit hexadecimal key that needs to be generated or created before attempting to communicate or synchronize an SDAC. Hexadecimal values range from 0-9 and A-F. Values outside these ranges will not work.

Communication Settings

Encryption Key

Please enter a properly formatted encryption key for the specified length.

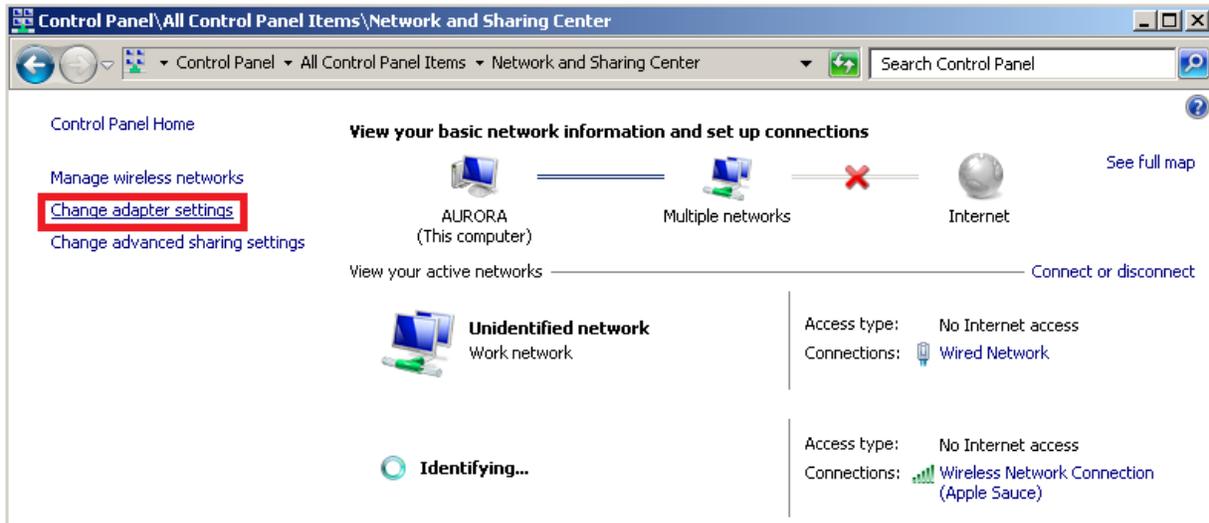
Doing a right click will display a *Generate* button that will create a key when clicked.

Communication Settings

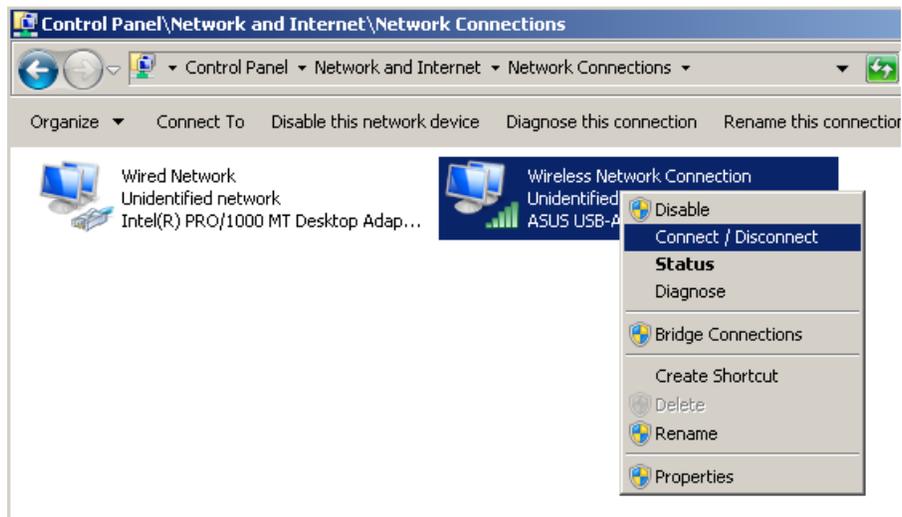
Encryption Key

AD-HOC (Peer to Peer) Connectivity

Go to Network and Sharing Center and click on *Change adapter settings*.



Right click on the wireless adapter and select *Connect/Disconnect*.



Look for the target SDAC in the list. It will be displayed as XpicoWiFi_xxxxxx, where the xxxxxx represents the last 6 digits of the SDACs MAC address. The security key to connect is XPICOWIFI.



Once connected, open a web browser and connect to <http://192.168.0.1>. You will then be prompted for a user name and password. The password is the serial number of the SDAC.

Lantronix only supports the latest version of Internet Explorer, Mozilla Firefox, Safari and Chrome browsers.



The Status window of the SDAC web portal will now be displayed.

Configuring an SDAC to Connect to a Wireless Network

Once connected to the SDAC, the first step is to update the *AES Credentials*. Click on *LunaCredential*.

The screenshot shows the LUNA Access Control Software interface. The main heading is "AES Credential Management". On the left is a navigation menu with items: Status, AES Credentials (selected), CLI Server, Clock, Device, Diagnostics, HTTP Server, Network, Tunnel, User, and WLAN Profiles. The main content area has a "View or Edit" button and a "Delete" button. Below these is a table with one entry: "LunaCredential" with a checkbox. A text input field labeled "Create new AES Credential" is present. On the right, there is a "[Logout]" button and a help text area explaining the page's functionality: "This page allows view, edit, delete or creation of an AES Credential on the device. Select a credential for editing by clicking its name; this takes you to the Configuration web page. Delete one or more credentials by checking their delete checkboxes. Create a new credential by entering a name in the text box. The new credential initially has empty keys. When you name a new credential or check a box, the Submit button will appear. Use the Submit button to update the credentials and save them to Flash." At the bottom, there is a copyright notice: "Copyright © dormakaba Canada Inc. 2018. All rights reserved." and a "help" link.

Copy the *Encryption Key* saved in Luna, on the *Settings* window and then paste it into the *Encrypt Key* and *Decrypt Key* fields on the SDAC. Hit the *Submit* button.

The screenshot shows the LUNA Access Control Software interface for the "AES Credential LunaCredential Configuration" page. The navigation menu on the left is the same as in the previous screenshot, with "AES Credentials" selected. The main content area has two text input fields: "Encrypt Key:" and "Decrypt Key:", both containing dotted lines. Below these fields is a "Submit" button. On the right, there is a "[Logout]" button and a help text area: "Each AES Credential holds a secret Encrypt Key and Decrypt Key for secure communication." At the bottom, there is a copyright notice: "Copyright © dormakaba Canada Inc. 2018. All rights reserved." and a "help" link.

To set a static IP address, click on *Network* in menu, and then highlight *wlan0*, *Interface*, and *Configuration* options. Enter the desired IP address and subnet mask. Gateways are only entered if required. Hostname, DNS and MSS are not support fields. Disable the DHCP client, as the SDAC will not act as a DHCP server in this mode. Hit the Submit to complete.

LUNA™
Access Control Software

Status [\[Logout\]](#)

ap0 wlan0

Interface Link

Status Configuration

Interface wlan0 Configuration

State: Enabled Disabled

DHCP Client: Enabled Disabled

IP Address:

Default Gateway:

Hostname:

Primary DNS:

Secondary DNS:

MSS: bytes

These settings pertain to the **Network Interface** on the device. To see the effect of these selections after a reboot, view the corresponding **Status**. **Changes will take effect after reboot or wake from sleep or standby.**

When ap0 is enabled, DHCP Server will assign IP addresses to ap0's clients. DHCP Server manages up to 4 simultaneous clients. (Only 3 if wlan0 is enabled.)

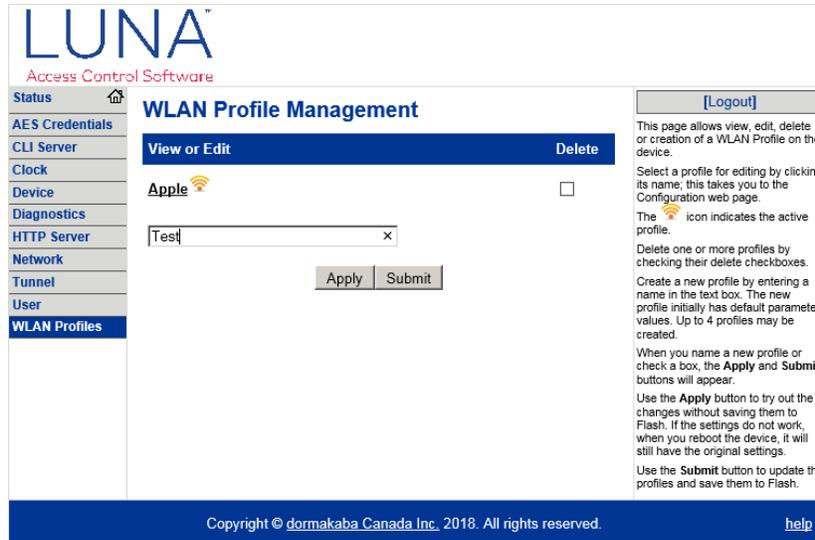
Copyright © [dormakaba Canada Inc.](#) 2018. All rights reserved. [help](#)

To avoid connection issues, it is advised to set a timeout value.

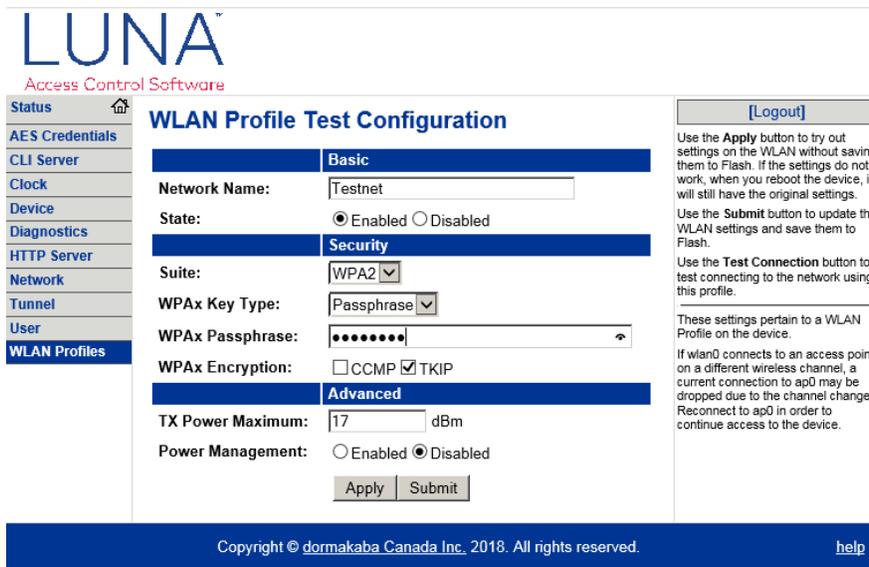
The screenshot displays the LUNA Access Control Software interface. On the left is a navigation menu with items: Status, AES Credentials, CLI Server, Clock, Device, Diagnostics, HTTP Server, Network, Tunnel (highlighted), User, and WLAN Profiles. The main content area is titled "Tunnel 1 Disconnect Configuration" and includes a summary box for "Tunnel 1" with buttons for Status, Accept, Connect, and Disconnect. Below this, the configuration settings are: Stop Character (set to <None>), Flush Stop Character (radio buttons for Enabled and Disabled, with Enabled selected), Modem Control (radio buttons for Enabled and Disabled, with Disabled selected), Timeout (input field with 60000 and label "milliseconds"), and Flush Line (radio buttons for Enabled and Disabled, with Disabled selected). A right-hand sidebar contains a [Logout] button and a note: "These settings relate to Disconnecting a Tunnel." The footer shows "Copyright © dormakaba Canada Inc. 2018. All rights reserved." and a "help" link.

NOTE: This value will be set in future SDAC units and may not require adjustment.

In the SDAC web portal, select the WLAN Profiles menu item. To connect to a network, you must first give the connection a name. Once a name is entered, hit the Apply button. Do not hit the Submit button until setup is completed.



Once the name appears in the list, click on it to edit the connection settings. Complete the connection settings per the network. Network Name is also called S.S.I.D and it is critical that it is accurate (like all other fields). Hit the Apply button to test the connection and Submit to complete.



Reboot the SDAC device and check connectivity.

Subnets

Class A

Network Bits	Subnet Mask	Number of Subnets	Number of Hosts
/8	255.0.0.0	0	16777214
/9	255.128.0.0	2 (0)	8388606
/10	255.192.0.0	4 (2)	4194302
/11	255.224.0.0	8 (6)	2097150
/12	255.240.0.0	16 (14)	1048574
/13	255.248.0.0	32 (30)	524286
/14	255.252.0.0	64 (62)	262142
/15	255.254.0.0	128 (126)	131070
/16	255.255.0.0	256 (254)	65534
/17	255.255.128.0	512 (510)	32766
/18	255.255.192.0	1024 (1022)	16382
/19	255.255.224.0	2048 (2046)	8190
/20	255.255.240.0	4096 (4094)	4094
/21	255.255.248.0	8192 (8190)	2046
/22	255.255.252.0	16384 (16382)	1022
/23	255.255.254.0	32768 (32766)	510
/24	255.255.255.0	65536 (65534)	254
/25	255.255.255.128	131072 (131070)	126
/26	255.255.255.192	262144 (262142)	62
/27	255.255.255.224	524288 (524286)	30
/28	255.255.255.240	1048576 (1048574)	14
/29	255.255.255.248	2097152 (2097150)	6
/30	255.255.255.252	4194304 (4194302)	2

Class B

Network Bits	Subnet Mask	Number of Subnets	Number of Hosts
/16	255.255.0.0	0	65534
/17	255.255.128.0	2 (0)	32766
/18	255.255.192.0	4 (2)	16382
/19	255.255.224.0	8 (6)	8190
/20	255.255.240.0	16 (14)	4094
/21	255.255.248.0	32 (30)	2046
/22	255.255.252.0	64 (62)	1022
/23	255.255.254.0	128 (126)	510
/24	255.255.255.0	256 (254)	254
/25	255.255.255.128	512 (510)	126
/26	255.255.255.192	1024 (1022)	62
/27	255.255.255.224	2048 (2046)	30
/28	255.255.255.240	4096 (4094)	14
/29	255.255.255.248	8192 (8190)	6
/30	255.255.255.252	16384 (16382)	2

Class C

Network Bits	Subnet Mask	Number of Subnets	Number of Hosts
/24	255.255.255.0	0	254
/25	255.255.255.128	2 (0)	126
/26	255.255.255.192	4 (2)	62
/27	255.255.255.224	8 (6)	30
/28	255.255.255.240	16 (14)	14
/29	255.255.255.248	32 (30)	6
/30	255.255.255.252	64 (62)	2