Location		
Locate Device Intel_2	4:42:8C 🗸 At Sep 9, 9;	11:59 AM Serif Location: //Locations/Unkn. Event Start Time: Sep 9, 9:11:56 AM Event End Time: Sep 9, 11:09:39 AM
		Floor Map View)
Locating Device		Distance from Locating Device
Device Name	[Sensor] AirTight_40.12 FB	e 25 50 75m
Location	Unknown	Land to the second
Tag		0 50 100 150 200 250 ft.
Device Name	[Sensor] AirTight_40.12.C8	a 25 50 25m
Location	raval	······
Tag		0 50 100 150 200 250 ft.
Device Name	[Sensor] AirTight_40.13:20	1 15 50 25m
Location	Unknown	
Tag		0 50 100 150 200 250 ft.
Device Name	[Sensor] Desk-347-Gamma	a 25 50 25m
Location	naval	
Tag		0 50 100 150 200 250 ft.
		Estimation as on: (Sep 9, 2009 8:11 AM)
		P

Location dialog

Note: The first row in the Client based threat displays the Event Time, while rest of the rows displays the Start/End Time of Association. This is valid for all Client based threats, **except Ad hoc**.

Client Based Threat – Prevention Tab

Prevention Tab shows the details of the Quarantine status of the association in the Association tab.

10		0				Location	Event Details		Cateo	Event Star	Event
523166	A		A	0	13	Location 1/N	Client [Intel_1D:4D:19	oligin	Miche	Feh Q R.	Eeb 9
23094	A	2	A	0	1	Location 1/Nod	Client Linknown Lis in Br	idoina/T	Mishe	Feb 9, 6:3	Feb 9
23021	-	a	Ă	0	10	Location 1/Nod	Client [unknown] is in Br	idoma/1	Mishe	Feb 9, 4:5	Feb 9
22555	A		Ã	õ	F	Location 1/Nod	Client [unknown] is in Br	idana/L.	Mishe	Feb 9. 4:0	Feb 9
22119	A	8	Ă	0	F	Location 1/Nod	Client [Intel 00:4E:3C] i	is in Bri	Misbe	Feb 8. 9:0	Feb 8
21995	A	8	Ā	G	富	Location 1/Nod	Client [Intel 00:4E:3C] i	s in Bri	Misbe	Feb 8, 5:5	Feb 8
21877	Δ	8	À	0	ñ	Location 1/Nod	Client [Intel_00:4E:3C] i	s in Bri	Misbe	Feb 8, 4:3	Feb 8,
			-	-	-				and the second second		and the second se
21438 Event St	A	ime:	Feb	9,8	1:08	Location 1/Nod :36 PM Ev	Client Junknown1 is in Br ent End Time: Feb 9, 8:1	nidaina/I	Misbe	Feb 7. 10:	Feb 7
21438 Event St. Associa	∆ art T tion	ime: Pr	Feb	9, 8	108	Location 1/Ned :36 PM Ev idmin	Client Funknown1 is in Br ent End Time: Feb 9, 8:1	ridaina/1	Misbe	Feb 7, 10:	Feb 7
21438 Event St. Associa	art T tion Clie	ime: Pr	Feb	9,8	1106 D	Location 1/Nod :36 PM Ev Idmin	Client Funknown1 is in Br ent End Time: Feb 9, 8:1 Association Start T)	nidaina/T 19:02 PM Associatio	Misbe	Feb 7. 10:	Feb 7
Event St. Associa	art T tion Clie AD:	ime: Pr int 20n	Feb	9,8	5106 n 4	Location 1/Nod :36 PM Ev sdmin AP	Client Funknown1 is in Br ent End Time: Feb 9, 8:1 Association Start T	ridaina/T 19:02 PM Associatio	Misbe	Feb 7. 10:	Feb 7
21438 Event St. Associa ntel 1D: ntel 1D:	A art T tion Clie AD: AD:	ime: Pr snt 20n 20n	Feb	9,8	5106 n 4	Location 1/Nod :36 PM Ev idmin AP 	Client Junknown1 is in Br ent End Time: Feb 9, 8:1 Association Start T Feb 9, 8:08:36 PM	Associatio	Misbe n End Tim 4:43 PM	Feb 7, 10;	rantine

Client Based Threat Details – Prevention Tab

The fields in **Prevention Tab** are as follows:

- Client
- AP
- Association Start Time
- Association End Time
- **Quarantine:** Specifies the action taken on both the devices in the association. Even if one of device is quarantined, the association is Quarantined, else it is Not Quarantined. Click **Quarantined**, the Quarantine Details dialog opens. Click **Not Quarantined**, the **Not Quarantined Reason** dialog opens.

Client Based Threat – Admin Tab

Admin Tab shows all the administrator actions taken on the Client during the Event Start Time and Event End Time.

ID ID ID ID 523166 △ △ △ □ Loc 523094 △ □ □ □ □ 523021 △ □ □ □ □ 522555 △ □ △ □ □ 522119 △ □ □ □ □	Location ation 1/Node123 ition 1/Node123 ition 1/Node123 ition 1/Node123	Event D Client [Client [Chent [Chent [Category Misbeha Misbehavi Misbehavi	Event Start Ti Feb 9, 8:08: Feb 9, 5:38:1 Feb 9, 4:51:2	Event Sto Feb 9, 8: Feb 9, 6:4 Feb 9, 5:0
523166 △ □ ↓ □ ↓ □ ↓ tor. 523094 △ □ ↓ ↓ □ ↓ □ ↓ □ ↓ ↓ ↓ □ ↓ □	ation 1/Node123 ation 1/Node123 ation 1/Node123 ation 1/Node123	Client [Client [Chent [Misbehavi Misbehavi	Feb 9, 8:08: Feb 9, 6:38:1 Feb 9, 4:51:2	Feb 9, 8: Feb 9, 6:4
523094 ▲ ↔ ▲ O → Loc 523021 ▲ ↔ ▲ O → Loc 522555 ▲ ↔ ▲ O → Loc 522119 ▲ ↔ ▲ O → Loc	ition 1/Node123 ition 1/Node123 ition 1/Node123	Client [Chent [Chent [Misbehavi	Feb 9, 5:38:1 Feb 9, 4:51:2	Feb 9, 6:4
523021 ▲ 🖾 🖨 O a Loc 522555 ▲ 🖾 🖨 O a Loc 522119 ▲ 🖾 🖨 O a Loc	ition 1/Node123	Chent [Misbehavi	Feb 9, 4:51/2	Feb 9, 5-0
22555 △ 🖂 🎝 Ο â Loc 522119 △ 🖂 🛱 Ο ā Loc	tion 1/Node123	Chent L			(
22119 🛆 🖂 🖨 🖸 🔂 Loca		and the second se	Misbeham	Feb 9, 4:06:4	Feb 9, 4:3;
the second se	ition 1/Node123	Client [1	Misbehavi	Feb 8, 9102:2	Feb 8, 9:5
21995 🛆 🖂 😂 🔂 🔂 Loci	tion 1/Node123	Client [1	Misbehay	Feb 0, 5:50:1	Feb 8, 8:2
521877 🛕 🖼 🚨 👩 Loca	tion 1/Node123	Çlient [L.,	Misbehavi	Feb 8, 4:31:4	Feb 8, 5:3
21438 🛆 🖂 🛱 🔂 🖬 Loca	tion 1/Node123	Client I	Misbehavi	Feb 7, 10:26:	Feb 7. 10:
event Start Time: Feb 9, 8:08:36 I	M Event End 1	Time: Feb 9, 8:1	19:02 PM		
Association Prevention Adm	n				
User	Action			Т	ime
dmin Removed device p	ntel_24:42:8C] from Qua	arantine		Feb 9, 8:18	:05 PM

Client Based Threat Details – Admin Tab

The fields in **Admin Tab** are as follows:

- User: Specifies the name of the user who took action on the threat.
- Action: Specifies the action taken by the user for the Client based threat, such as Client added to quarantine, Client name changed.
- Time: Specifies the time when the user action was taken

Note: Client Based Threat – Misassociation, Unauthorized Association, Bridging Client, and Banned Client have the same fields for the tabs **Association**, **Prevention**, and **Admin**. However Client Based Threat – Ad hoc has some different fields as discussed in the section below.

Client Based Threat – Ad hoc

Client – Ad hoc Threat displays only all the Clients participating in the Ad hoc connection.

To open the **Client – Ad hoc Threat Details** dialog, select the **Client – Ad hoc threat** row on the **Forensics** screen, and click **Details**. The **Client – Ad hoc Threat Details** dialog opens.

S23076 S <th>ID</th> <th></th> <th></th> <th></th> <th>1</th> <th>Location</th> <th></th> <th>Event Details</th> <th>Categ</th> <th>Event Star</th> <th>Event</th> <th>]</th>	ID				1	Location		Event Details	Categ	Event Star	Event]
S22322 Image: S223222 Image: S223222	23076	0	-	0 8	8	Location 1/Nod	An Ad hoc	network [vivek] invol	Ad ho	Feb 9, 610	Feb 9,	1
221511 Image: Construction of the second	22822					Location 1/Nod	An Ad hoc	network [adhocnetwon]	Ad hour	Feb 8, 111.	Feb 9.	
S21509 Image: Section of the sectin of the section of the section of the section	21511	•		0 8	i i	Location 1/Nod	An Ad hos	network [damn_dhis]	Ad ho	Feb.8, 1:0	Feb B	
S2491 S S T //Locations/Lin An Ad hoc network (vvv) involvi Ad ho Feb 5, B:1 Fet 5, B:1 Fet 5, B:1 Feb 5,	21509			0 *		Location 1/Ned	An Ad hoc	network [damn_this]	Ad ho	Feb B; 1:0	Feb Ø,	
139968 Image: Second secon	52491	ě.		6 s	-	//Locations/Un	An Ad hoc	network (vvv) involvi	Ad lio	Feb 5, 8:1	Feb 5	
139965 Image: Start Time: Feb 2, 5:29:46 PM Event End Time: Feb 2, 6:31:02 PM Association Prevention Admin Client Association Start Time Association End Time Locate	39968					//Locations	An Ad ho	c network [Internet	Ad ho	Feb 2, Stin	Feb 2	
Image: Start Time: Feb 2, 5:29:46 PM Event End Time: Feb 2, 6:31:02 PM Association Prevention Admin Client Association Start Time Association End Time	39965	•	-	6 s		//Locations	An Ad hop	network [InternetCon	Ad ho	Feb 2, 5:2	Feb 2	
Image: Peb 2, 5:29:46 PM Event End Time: Feb 2, 6:31:02 PM Association Prevention Admin Client Association Start Time Association End Time	19661	6		<u>n *</u>	1	//Locations	An Ad hoc	network [internetCon	Ad how	Feb 2, 4:5	Feb Zin	
Ivent Start Time: Feb 2, 5:29:46 PM Event End Time: Feb 2, 6:31:02 PM Association Prevention Admin Client Association Start Time Association End Time Locate										4 1 1	0.40	2
Client JI Association start time JI Association End time JI Locate		-			-	Accession for fr	ut Time	Accession Fed To		1.640		-
Intel 01:E9:13 Feb 2, 5:29:46 PM Feb 2, 5:32:39 PM Locate	te) 01:8	E9:1	3		_	Feb 2, 5:29:46 PM	arc mine	Feb 2, 5:32:39 PM	ite ite	scate	(e	-
Intel BF:D6:27 Feb 2, 5:29:46 PM Feb 2, 6:31:02 PM Locate	tel BE:0	D6:2	7			Feb 2, 5:29:46 PM	0	Feb 2, 6:31:02 PM	L.	ocate		
unknown Feb 2, 5:29:46 PM Feb 2, 6:31:02 PM Locate						Feb 2, 5:29:46 PM		Feb 2, 6:31:02 PM	L	ocate		
	hknown							and the state of t				

Client - Ad hoc Threat Details dialog



Client Ad hoc Threat - Association tab

The fields in Association Tab are as follows:

- Client
- Association Start Time
- Association End Time
- Locate: Click Locate, the Location dialog opens. In this case only the Client name appears in the Locate Device drop down list. Select Start Time of Ad hoc Connection and End Time of Ad hoc Connection from At drop down list. Click Locate the location of the selected device at the selected time is displayed.

Client Ad hoc Threat - Prevention tab

Click on **Prevention Tab** in the Client – Ad hoc Threat Details dialog.

523076				Location	Event De	tails	Categ	Event	Star	Event
	• •	0	8	Location 1/Nod	An Ad hoc network.	[vivek] invol	Ad ho	Feb 9.	610,	Feb 9,
22822	• =		8	Location 1/Nod	An Ad hoc network	[adhocnetwo	Ad ho	Feb B.	11.00	Feb 9m
21511	• 🖘	0	8	Location 1/Ned	An Ad hoc network	[damn_this]	Ad ham	Fab 8	1:0.00	Fab alim
21509	• 👄	8	*	Location L/Ned	An Ad hoc network	[damn_this]	Ad ho	Feb 8.	1.0	Feb S.m
52491	0 🖂			//Locations/Un	An Ad hoc network	[vvv] mvolw	Ad hu	Feb S.	8:1	Feb 5,
39968	• •	0		//Locations	An Ad hoc netwo	k [Internet	Ad ho	Feb 2	5im	Feb 2
139965	• 👄	6		//Locations	An Ad hoc network	InternetCon.	Àd họ - i	Feb 2.	512	Feb 2
139661		12	8	//Locations	An Ad hoc network	[InternetCon	Ad how	Feb 2.	45	Feb 2
								4	1 1	0+0 6
	Client			Addition Start T	Association End Time	0	0	ration		_
Intel 01:ES	9:13	_	Fel	2. 5:29:46 PM	Feb 2, 5:32:39 PM	Not Ouarantio	ed be	gnuire		
Intel BF:D	6:27		Feb	2, 5:29:46 PM	Feb 2, 6:31:02 PM	Not Quarantin	ed			
unknown		_	Feb	2, 5:29:46 PM	Feb 2, 6:31:02 PM	Not Quarantin	ed			
				the second se	and the second se					

Client – Ad hoc Threat Details – Prevention tab

The fields in **Prevention** tab are as follows:

- Client
- Association Start Time
- Association End Time
- Quarantine: Specifies quarantine action taken on the devices during the Ad hoc connection. Click Quarantined, the Quarantine Details dialog opens. Click Not Quarantined, the Not Quarantined Reason dialog opens.

Client Ad hoc Threat - Admin Tab

Click on **Admin Tab** in the Client – Ad hoc Threat Details dialog.

ID					Location	Event Details	Category	Event Start Ti Event Sto.
23076		-		â	Location 1/Nod.	An Ad hoc network [vin-	Ad hoc N	Feb 9, 6:06:0 Feb 9, 0
2322	•		ê (8		Location 1/Nod	An Ad hoc network [ad	Ad hoc N	Feb 8, 11:40 Feb 9, 12.
21511	۲	-	8	1	Location 1/Nod	An Ad hoc network [da	Ad hoc N	Feb 8, 1:05:1., Feb 8, 11-
21809		-		đ	Location L/Nod.	An Ad hoc network [da	Ad hoc No.	Feb 6, 1:03(1.) Tab 8, 1())
52491	•				//Locations/Un	An Ad hoc network [vv	Ad Noc N	Feb 5, 8:17/2 Feb 5, 8
39968	•		6 *		//Locations	An Ad hoc network [Ad hor N	Feb 2, 5:29: Feb 2, 6:
39965	•				//Locations	An Ad hoc network [1n	Ad hoc N	Feb 2, 5:29:2 Feb 2, 51
39661				18	//Locations	An Ad hoc network [In	Ad hoc Nee	Feb 2, 4:59:1 Feb 2, 51
Event St	tion	Pre	venti	on	Admin			
Event St Associa	tion	Pre	venti	on	Admin	Action	_	Time
Event St Associa Use idmin	tion tion	Pre	venti hange	d den	Admin ice name from (Net	Action gear_CA:DF:83] to [vivek]		Time **

Client - Ad hoc Threat Details - Admin tab

The fields in **Admin** tab are as follows:

- User
- Action: Displays all the actions taken on *all the Clients* participating in the Ad hoc connection
- Time

Forensics Tab – User Saved Settings

The following User choices made during browsing of Forensics Tab are saved by the system.

• Time Filter

These settings are saved on log out as well as movement to other tabs on the Console.

Administration Tab

Introduction

The system is highly customizable and can be configured to suit the needs of your enterprise. The Administration screen allows you to perform various administrative activities such as event, device, and user management, configure the system and location settings, and enable integration with SAFE and third party applications.

Administration Screen

The **Administration** screen includes two panes.

On the left, you see policy groups categorized into global policies and local policies; Global policies are grouped under the **Global** tab while Local policies are grouped under the **Local** tab.

On the right, you see the details of the selected policy node. The following figure displays the Administration tab.

Clobal Clices Clobal Policies Clobal Policies Clic Event Settings Clic User Management Clic User Management Clic Settings Clic	Global Policies Global Policies include system settings that are applicable to all locations defined in SpectraGuard Enterprise. These policies cannot be controlled separately per location. Global policies can be modified only by users with appropriate permissions.	
WLAN Integration Why ESM Integration SpectraGuard SAFE	Define device settings.	*
	User Management Manage the users who will access SpectraGuard Enterprise.	
	Location Settings Settings to control location tracking, live RF views and RF computation for each location.	
	System Settings Configuration for system settings.	
	WLAN Integration Configure settings for integration with third party WLAN management systems.	
	Enterprise Security Management (ESM) Integration Configure settings for Server to integrate with external Enterprise Security Management (ESM) systems.	
	SpectraGuard SAFE Configure policies to push to Clients running SpectraGuard SAFE.	

Global tab

📰 Dashboard 💇 Events 🔯 Devices	n Locations 🕃 Reports 🔊 Forensics 🌌 Administration	Aug 10 2011, 11:31:37 AM (GMT +0530) 😰 🕐 🚍 💽
🛱 Global 🛱 Local	Selected Location: //Locations/Unknown	Events On Prevention Off
O Locations C Unknown C Unknown C California C California C California C California C California	Local Policies Local Policies can be modified on a per-loc either custom defined or inherited (as a gr Policy definition for a selected location is parent location are propagated downward, definition the selected location is not inherit	ation basis. Local policies consist of policy groups. All policies within a policy group can be oup) from the parent location. By default, all policies are inherited. Inherited Policies: herited from the policy definition at the parent location. Any changes to the policy of the Customize Policies: Policy definition is customized for a selected location. The policy ted from the parent location.
Image: Contract of the second seco	Wireless Policies Configuration of your authorized wireless setup.	Customize
Event Settings AP Configuration Sensor Configuration Sensor Configuration Location Properties	Operating Policies Customize the AP and Client auto-classification behavior. Define the p	policies for intrusion prevention.
	Event Settings Define event related settings at each location.	🛱 Customize
	AP Configuration Manage AP configuration templates. These templates control AP oper	ation parameters.
	Sensor Configuration Manage Sensor configuration templates. These templates control Sen	sor password, channel selection and antenna connections.
	Location Properties Customize activation flags and device list locking flags at selected I	ocstion.

Local Tab

Global Policies

Global policies are the policies that are applicable to the entire system. A superuser or an administrator with rights to the root location can modify the global policies.

Click the Global tab on the Administration screen to view the policies groups under this tab.

Event Settings

The Event Settings option enabled you to configure the following event settings in the system.

- Hotspot SSID's
- Event Regeneration
- Vulnerable SSID's

Vulnerable SSID

APs have well known default SSIDs and many users may not change these SSIDs when deploying the APs. Therefore it is highly likely that APs using default SSIDs are present in the enterprise neighborhood. If an enterprise Client probes for a default SSID, it is at risk of connecting to the neighborhood AP without the user necessarily knowing about it. Also if an enterprise AP uses a default SSID, such an AP may attract undesirable Clients to connect to it. If you consider an SSID to be vulnerable to hackers, you can open the **Vulnerable SSIDs** screen and enter the SSID under **SSID (ASCII character string)**. Click **Add** and then **Apply** to place the SSID in your database. If an AP point with a vulnerable SSID is detected, the system generates an event.

Note: Commonly known SSIDs are listed by default. To enter a blank SSID: no string, click <*Add*> without entering any text. The list shows the SSID as NULL.

Remove SSIDs from this list by selecting the SSIDs and clicking Delete. To remove the SSIDs from the database, click Apply.

📰 Dashboard 💇 Events 🍐 Devices 🊷	Locations 📑 Reports 🔊 Forensics 🌉 Administration 🥳	Jun 13 2011, 10:25:27 AM (GMT +0530) 😰 🔞 든 💽 📆
💯 Global 🗊 Local	📵 Vulnerable SSIDs	
Dashboard V Events & Devices Clobal V Local Clobal Policies Clobal Policies Valuerable SSIDs Regeneration Valuerable SSIDs User Management Science Settings Valuer Management Science Settings Valuer Management Science Settings Science	Locations	Jun 13 2011, 10:25:27 AN (GMT +0530) 2 (2) (2) (2) (2) (2) (2) (2) (2) (2)
	Click Apply to save the list of vulnerable SSIDs.	

Vulnerable SSIDs

Regeneration

Some events are generated repeatedly when the cause persists; for example, Denial of Service (DoS) (Security) and traffic events (Monitoring).

The **Regeneration** screen enables you to specify how often an event is repeated if the cause persists under the **Event Regeneration Interval**.

(Minimum: 1 hour; Maximum: 168 hours; Default: 24 hours)

📰 Dashboard 💇 Events 🧔 Devices 🤞	Locations 📴 Reports 🔊 Forensics 🌆 Administration	Jun 13 2011, 10:29:27 AM (GMT +0530) 😰 🕐 든 💽 🕂
🛱 Global 🛱 Local	🔞 Event Regeneration Interval	
	Event Regeneration Interval	
Clobal Policies Event Settings Vulnerable SSIDs	Certain events are generated repeatedly if the cause for the event continues to persist for a long time. Select how often such an event should be generated if its cause continues to persist.	
Regeneration Hotspot SSIDs	Event Regeneration Interval 24 C hours [1-168]	
Device Settings	Apply Cancel Restore Defaults	
Ver Management Ver Management Ver Management Ver System Settings Ver Management Ver System Settings Ver Management Ver System Settings Ver System Settings Ver System Settings		

Event Regeneration Interval

Hotspot SSIDs

It is highly likely that hotspot APs are present in the enterprise neighborhood. If enterprise Client probes for well known hotspot SSID, it is at risk of connecting to the hotspot AP without the user necessarily knowing about it. Also if enterprise AP uses hotspot SSID on it, such an AP may attract undesirable Clients to connect to it. If you consider an SSID to be vulnerable to hackers, you can open the **Hotspot SSIDs** screen and enter the SSID under **SSID (ASCII character string)**. Click **Add** and then **Apply** to place the SSID in your database. If an AP with a vulnerable SSID is detected, the system generates an event.

Note: The system lists commonly known SSIDs by default. To enter a blank SSID: that is, with no string, click *<Add>* without entering any text. The list shows the SSID as NULL.

Dashboard 2 Events Devices	Cocations Reports Corensics Administration	Jun 13 2011, 10:46:27 AM (GMT +0530) 🔮 🕐 🧱 🤇
Global 🗊 Local	Hotspot SSIDs	
	Hotspot SSIDs	
Global Policies	List of Hotspot SSIDs	
Event Settings	It is highly likely that hotspot APs are present in the enterprise neighborhood. If enterprise Client prob- known hotspot SSID, it is at risk of connecting to the hotspot AP without the user necessarily knowing or Also if enterprise AP uses hotspot SSID on it, such an AP may attract underisable Clients to connect to	es for well sbout it. it.
Regeneration Hotspot SSIDs	SSID (ASCII character string) Define the list of hotspot SSIDs. Commonly known hotspot SSIDs have already been pre-filled.	
La Device Securgs	Ambure Delete	
So oser Hanagement		
Cocation Settings	AVV	
E System Settings	bestouy	
WLAN Integration	pongo	
ESM Integration	boldstreet	
SpectraGuard SAFE	BTopenzone	
	Cancel Restore Defaults	

Hotspot SSIDs

Remove SSIDs from this list by selecting the SSIDs and clicking **Delete**. To remove the SSIDs from the database, click **Apply**.

Device Settings

Smart Device Type

You can view, add, and delete the smart device types using the **Smart Device Type** dialog. Go to **Administration** >**Global->Device Settings->Smart Device Type** to view the **Smart Device Type** dialog. The dialog shows the system-defined smart device types , and the user-defined smart device types, if any. The following figure shows the **Smart Device Type** dialog.

📰 Dashboard 💇 Events 💊 Devices 📢	Locations 📴 Reports 🔍 Forensics 🌉 Administration	2	Sep 22 2011, 12:01:46 PM (GMT -0400) 📝 😨 🗐 🖁
🛱 Global 🗊 Local	Smart Device Type		
Global Policies Global Policies Control Settings Control Settings Smart Device Type	Smart Device Type Smart Device Type allows users to add and delete sm. Users can add new Smart Device types and delete the Note that System added Smart Device Types cannot b Smart Device Type iPhone	art device types. manually added types, e removed. Add	
Import Devices Thresholds Discovery Banned AP List Banned AP List Banned Client List User Management System Settings W VLAN Integration W LAN Integration W SpectraGuard SAFE	iPodTouch iPad Blackberry Android Nokia Motorola Samsung HTC		

Smart Device Type

Adding a smart device type

To add a new smart device type, click **Add**. Enter the **Smart Device Type** in the **Add Smart Device Type** dialog shown below, and click **OK** to add the smart device type to the existing list of smart device types.

Add Smart Device Type	
Smart Device Type]
OK Cance	

Add Smart Device Type

Deleting a smart device type

You can delete only the smart device types that have been manually added using **Devices->Clients->Categorized-> Authorized->Smart Device->Change Device Type** or through the **Add Smart Device Type** dialog. You cannot delete the system-defined smart device types.

To delete a user-defined smart device type, select the smart device type and click **Delete**. Click **Yes** to confirm the deletion.

Confirm	
?	Devices of this Smart Device Type will be categorized as Unknown and the type will be permanently removed from the system. Are you sure you want to delete this Smart Device type?

Delete Smart Device Type

Import Devices

Importing an Authorized AP List and an Authorized or Non-authorized Clients List is an efficient alternative to manual movement of these devices into the Authorized/Non-authorized bins. After successfully importing these lists, the system automatically classifies the APs and Clients in the respective lists as Authorized/Non-authorized.



Import Devices

You can move Authorized APs to the Authorized folder using one of the following methods:

- Move an AP to the Authorized folder using right click and Move option
- Import the Authorized AP list
- Synchronize with an AP Management server

Note: Once you move an AP to the *Authorized* folder, the system *never* automatically removes it from the *Authorized* folder, even if it later detects that the AP is *unwired* from the enterprise network.

a manufactory.					
Auto Tag Devices	🕈 🔘 Manually Tag Dev	ices to:		Change	
inter AP details**			Authorized AP Import Lis	t**	
MAC Address	IP Address	Name	MAC Address	IP Address	Name
Add to List >>> *MAC address, IP addre nd device seperated by aste the list.	ess and name separated b new line. Use Ctrl+V to	ry tab	Delete **This list de	oes not display previously	imported Authorized A
Add to List >>> **MAC address, IP addre ind device seperated by aste the list. Dr Add AP details from Fil Add to List >>>	ess and name separated b new line. Use Ctrl+V to le Browse	y tab	Delete **This list d	oės not display previously	imported <i>Authorized A</i>

Under Import AP List, click Import Authorized AP List to open Import Authorized AP List dialog.

Import Authorized AP List

In the Import Authorized AP List dialog:

Under Tag Devices, select one of the following:

- **Auto Tag Devices:** To automatically tag the AP to the corresponding location.
- Manually Tag Devices to: Click Change to manually tag the AP to the desired location.

Under Enter AP details

- To add an AP's details, type the AP's MAC address, IP Address, and Name and click Add to List.
- To add an AP's details from a file, click **Browse**. On the **Select Authorized AP_Device_List_File** dialog, select the .txt file from the desired location and click **Open**. Then click **Add to List>>>**

Under Authorized AP Import List

- To delete an AP's details, select the corresponding row and click Delete.
- To import Authorized APs from the Authorized AP Import List, click OK

Note: When you import APs from a list, policy settings in the Setup Wizard do not affect these APs.

In the Import Devices dialog, under Import Client List, click Import Authorized Client List to open Import Authorized Client List dialog, click Import Guest Client List to open Import Guest Client List dialog, click Import Rogue Client List to open Import Rogue Client List dialog.

In the Import Authorized/Guest/Rogue Client List dialog:

Under **Tag Devices**, select one of the following:

- Auto Tag Devices: To automatically tag the Client to the corresponding location.
- Manually Tag Devices to:: Click Change to manually tag the Client to the desired location.

ually Tag Devices to:	Guest Client Import	Changaur List** IP Address	Name
Address Name	Guest Client Import MAC Address	List**	Name
Address Name	MAC Address	IP Address	Name
ime separated by tab	Delete **This I	ist does not display previously	/ imported Guest Clien
owse	l, this list cannot be reviewe	d.	
	nme separated by tab Use Ctrl+V to rowse Client Import List. Once saved	Delete **This I Delete **This I Use Ctrl+V to rowse Client Import List. Once saved, this list cannot be reviewe ported using this list, delete them from Devices screen.	Towse Client Import List. Once saved, this list cannot be reviewed.

Import Guest Client List

Under Enter Client details

- To add a Client's details, type the Client's MAC Address, IP Address, and Name and click Add to List>>>
- To add a Client's details from a file, click **Browse**. On the **Select Authorized/Guest/Rogue Client_Device_List_File** dialog, select the .txt file from the desired location and click **Open**. Then click **Add to List**.

Note: When you import sensors from a list, you can delete these sensors only from the Devices screen.

Under Authorized/Guest/Rogue Client Import List

- To delete a Client's details, select the corresponding row and click Delete.
- To import Authorized/Guest/Rogue Clients from the Authorized/Guest/Rogue Client Import List, click OK.

Note: When you import Clients from a list, policy settings in the Setup Wizard do not affect these Clients.

In the **Import Devices** dialog, under **Import Sensor List**, click **Import Sensor List** to open the **Import Sensor List** dialog:

In the **Import Sensor List** dialog:

Under **Tag Devices**, select one of the following:

- Auto Tag Devices: To automatically tag the sensor to the corresponding location.
- **Manually Tag Devices to:** Click **Change** to manually tag the sensor to the desired location.

Under Enter Sensor details

- To add a sensor's details, type the sensor's MAC address and Name and click Add to List>>>.
- To add a sensor's details from a file, click **Browse**. On the **Select Sensor_Device_List_File** dialog, select the .txt file from the desired location and click **Open**. Then click **Add to List>>>**.

Under Authorized Sensor Import List

- To delete a sensor's details, select the corresponding row and click **Delete**.
- To import sensors from the **Sensor Import List**, click **OK**.

Note: When you import sensors from a list, you can delete these sensors only from the Devices screen.

Thresholds

Threshold settings determine the status of devices in terms of up-down association and connectivity. The **Thresholds** screen enables you to set parameters for APs, clients, and sensors.



Device Thresholds

Device Threshold Parameters contains the following settings:

- AP Timeout
 - **Activity Timeout**: If the system senses no activity of the AP for the period specified here, it declares the AP inactive.

(Minimum: 60 seconds; Maximum: 600 seconds; Default: 300 seconds)

- Client Timeouts
 - **Activity Timeout**: If the system senses no activity from a Client for the period specified here, it declares the Client inactive.

(Minimum: 120 seconds; Maximum: 1200 seconds; Default: 600 seconds)

 Association Timeout: If the system sees no communication between an associated AP and Client pair for the period specified here, it declares the association as timed out.

(Minimum: 120 seconds; Maximum: 1200 seconds; Default: 600

- Sensor Parameters
 - **Maximum Number of Sensors Allowed**: Maximum number of sensors allowed to connect to the system at a given time.

(Maximum value is governed by the license applied and is a Read-Only field.)

• **Sensor Timeout**: The sensor sends keep alive information to the server at a regular time interval specified here, to tell the server that it is alive. If the system does not receive this keep alive information for a time span specified here, it declares the sensor inactive.

Note: Sensor timeout is not user configurable for this release and has been fixed as 600 seconds.

• **RF Signal Computation Constants**

Moving Average Constant: A constant used to find the weighted average of signal strength as seen by a sensor for a transmitter. Higher value gives more weight to more recently seen signal strength values.
 (Minimum: 0; Maximum: 1; Default: 0.05)

sensor observes signal strengths as RSSI reported by the driver. The system converts this information to dBm values for further use. The conversion formula for this is different for 2.4 GHz and 5 GHz frequency spectrum. The formula is dBm = RSSI + dBm Conversion Constant.

- RSSI <-> dBm Conversion Constant for 802.11a: This value used for 5 GHz band is set to -98.
- RSSI <-> dBm Conversion Constant for 802.11b/g: This value used for 2.4 GHz band is set to -90.
- Sensor Server Communication
- **Frequency of Device Updates**: The system is informed immediately when device attributes change or when a device is first detected. If no such changes take place, the system should still be informed about the device updates. Here you can set that time after which the system is notified of the updates.

(Minimum: 1 day; Maximum: 365 days; Default: 36 days)

• **Frequency of Signal Strength Updates**: The system should be periodically informed about the signal strength updates. Here you can set that time after which the system is notified.

(Minimum: 1 minute; Maximum: 5 minutes; Default: 2 minutes)

- **Records Constants (per Sensor):** A sensor maintains records for APs, Clients, and associations. The constants below define the maximum number of APs, Clients, and associations for which to maintain records with the sensor(s).
- Maximum Number of AP records to keep: Specifies the maximum number of APs for which to maintain records with the sensor(s).

(Minimum: 100; Maximum: 500; Default: 128)

 Maximum Number of Client records to keep: Specifies the maximum number of Clients for which to maintain records are with the sensor(s).

(Minimum: 100; Maximum: 500; Default: 256)

 Maximum Number of Association records to keep: Specifies the maximum number of associations for which to maintain records with the sensor(s).

(Minimum: 100; Maximum: 500; Default: 128)

Discovery

Sensors and NDs inject discovery (ARP) broadcast packets in bursts on the network at regular intervals. These packets detect the presence of wireless devices connected to the network. If there are multiple sensors and NDs on a subnet, only one injects discovery packets on the subnet.

📰 Dashboard 💇 Events 🏑 Devices 🌰	Locations 🔡 Reports 🔊 Forensics 🌆 Administration		Sep 22 2011, 12:11:18 PM (GMT -0400) 😰 🕐 🚍 💽 📆
🛱 Global 🗊 Local	🛋 Advanced - Device Discovery Param	eters	
	Device Discovery Parameters		
Clobal Policies Clobal Policies Content Settings Content Settings Smart Device Settings Import Devices The Thresholds	SpectraGuard Sensors and Network Detectors inject network at regular intervals. These packets are use connected to the network. If there are multiple Sen will inject discovery packets on the subnet. This screen defines the characteristics of these disc determines how guickly rogue devices can be detect		
- Discovery	Number of packets in a discovery burst		
Banned AP List	This parameter defines the number of packets sent	t in each discovery burst.	
Banned Client List	Number of packets in a discovery burst	300 \$ [10-1000]	
User Management			
E 🕻 System Settings	Time interval for packets in a discovery bur	st	
HILAN Integration	This parameter defines the time interval at which p		
 Wey ESM Integration SpectraGuard SAFE 	Time interval for packets in a discovery burst	50 💲 milliseconds [10-110]	
	Time to wait between two discovery bursts		
	This parameter determines the time to wait betwe the time taken to detect rogue devices connected	en two discovery bursts.This time also determines to your network.	
	Time to wait between two discovery bursts	75 🗢 seconds [3-1200]	
	Cancel Restore Defaults		

Device Discovery

The following options are available:

• Number of packets in a discovery burst: Specifies the number of packets that the system sends in each discovery burst.

(Minimum: 10; Maximum: 1000; Default: 300)

• Time interval for packets in a discovery burst: Specifies the time interval between two consecutive packets sent in a discovery burst.

(Minimum: 10 milliseconds; Maximum: 110 milliseconds; Default: 50 milliseconds)

• Time to wait between two discovery bursts: Specifies the time interval between two consecutive discovery bursts. This time also determines the time taken to detect rogue devices connected to your network. More the time to wait between two discovery bursts means more time is required to detect the connectivity of the wireless devices.

(Minimum: 3 seconds; Maximum: 1200 seconds; Default: 75 seconds)

Banned AP List

The **Banned AP List** dialog enables you to import a list of banned APs to the database. You define the wireless MAC addresses of APs that are blacklisted in your organization. If APs with these MAC addresses become visible, the system generates an alert.

Clobal D Local Banned AP List	
Banned AP List	
Interface Import Device Settings Device Settings Import Device Settings Device Settings Import Device Settings Device Settings	

Banned AP List

In the Banned AP List under Enter AP MAC addresses, enter the MAC address of a prohibited AP and click **Add to List>>>>**. The MAC address is added to the Banned AP List. You can also

- Use Ctrl + V to paste a list
- Add the MAC addresses from a file by clicking Browse and then selecting the file

Note: Separate MAC addresses by a comma, space, tab, semicolon, or new line.

Banned Client List

The **Banned Client List** dialog enables you to import a list of banned Clients to the database. You define the wireless MAC addresses of Clients that are blacklisted in your organization. For example, such MAC addresses could belong to laptops of employees who are no longer with the organization. If Clients with these MAC addresses become visible, the system generates an alert.

Banned Client List

In the Banned Client List under Enter Client MAC addresses, enter the MAC address of a prohibited Client and click <Add to List>>>>. The MAC address is added to the Banned Client List. You can also

- Use Ctrl + V to paste a list
- Add the MAC addresses from a file by clicking Browse and then selecting the file

Note: Separate MAC addresses by a comma, space, tab, semicolon, or new line.

User Management

Select the **User Management** option to set various user settings. You can manage different types of users, set the password and account locking policies.

The system allows you to configure and manage local users. The system also allows you to configure users, authenticated using LDAP and RADIUS. You can also set the user preferences for local users.

Users

The Users screen enables you to add, edit, and delete user accounts.

Initiality Local Image Spin Manage Spin Image Spin Manage Spin Image Spin Manage Spin Image Spin Image Spin Image Spin Ima	bectraGuard Enterprise to caraGuard Enterprise to Login ID mbozeman mkelly jeckert nhadad dmazza shelsby aozimek dfields agreen chayes admin trnanning	Ise Users Users. Double click t First Name Mark Michael John Nicholas David Steve Adam Dan Andrew Chris	b update user details. Last Name Bozeman Kelly Eckert Hadad Mazza Helsby Ozimek Fields Green	Access Rights //ADT //ADT //ADT //ADT //ADT //ADT //ADT //ADT	Session Timeout Never Expires Never Expires Never Expires Never Expires Never Expires Never Expires	Disabled? No No No No	[Total: 17 Suspended? No No No No
Global Policies Manage Sp. Colobal Policies Manage Sp. Colobal Policies Manage Sp. Device Settings 2 User Nanagement 2 User Nanagement 2 Password Policy 2 Password Policy 2 Account Suspension 2 User Preferences 2 User Preferences 2 User System Settings 2 User WLAN Integration 2 ESM Integration 2	ectraGuard Enterprise (Login ID mbozeman mkelly jeckert nhadad dmazza shelsby aozimek dfields agreen chayes admin trnanning	Michael John Nicholas David Steve Adam Dan Andrew Cchris	b update user details. Last Name Bozeman Kelly Eckert Hadad Mazza Helsby Ozimek Fields Green	Access Rights //ADT //ADT //ADT //ADT //ADT //ADT //ADT	Session Timeout Never Expires Never Expires Never Expires Never Expires Never Expires Never Expires	Disabled? No No No No No	[Total: 1; Suspended? No No No No
Image of the settings Image of the settings Image of the settings Image of the settings <t< th=""><th>Login D hugin D mbozeman mkelly jeckert nhadad dmazza shelsby aozimek dfields agreen chayes admin trnaning</th><th>First Name Mark Michael John Nicholas David Steve Adam Dan Andrew Chris</th><th>Last Name Bozeman Kelly Eckert Hadad Mazza Helsby Ozimek Fields Green</th><th>Access Rights //ADT //ADT //ADT //ADT //ADT //ADT //ADT</th><th>Session Timeout Never Expires Never Expires Never Expires Never Expires Never Expires Never Expires</th><th>Disabled? No No No No No</th><th>No No No No No No</th></t<>	Login D hugin D mbozeman mkelly jeckert nhadad dmazza shelsby aozimek dfields agreen chayes admin trnaning	First Name Mark Michael John Nicholas David Steve Adam Dan Andrew Chris	Last Name Bozeman Kelly Eckert Hadad Mazza Helsby Ozimek Fields Green	Access Rights //ADT //ADT //ADT //ADT //ADT //ADT //ADT	Session Timeout Never Expires Never Expires Never Expires Never Expires Never Expires Never Expires	Disabled? No No No No No	No No No No No No
Event Settings Image: Constraint of the setting of	bogin D mbozeman mkelly jeckert nhadad dmazza shelsby aozimek dfields agreen chayes admin trnanning	Mark Michael John Nicholas David Steve Adam Dan Andrew Chris	Last Name Bozeman Kelly Eckert Hadad Mazza Helsby Ozimek Fields Green	Access rights //ADT //ADT //ADT //ADT //ADT //ADT //ADT	Never Expires	No No No No No	No No No No
Device Settings 2 User Nanagement 2 LDAP 2 ADJUS 2 Password Policy 2 Account Suspension 2 Location Settings 2 System Settings 2 Werk Natagration 2 With Natagration 2 With Suspension 2 System Settings 2 With Suspension 2 With Suspension 2 With Natagration 2 With Suspension 2	nkelly jeckert nhadad dmazza shelsby aozimek dfields agreen chayes admin trnanning	Michael John Nicholās David Steve Adam Dan Andrew Chris	Kelly Eckert Hadad Mazza Helsby Ozimek Fields Green	//ADT //ADT //ADT //ADT //ADT //ADT //ADT	Never Expires Never Expires Never Expires Never Expires Never Expires	No No No No	No No No
Wiser Nanagement Image: Constraint of the second	jeckert nhadad dmazza shelsby aozimek dfields agreen chayes admin trianning	John Nicholas David Steve Adam Dan Andrew Chris	Eckert Hadad Mazza Helsby Ozimek Fields Green	//ADT //ADT //ADT //ADT //ADT //ADT	Never Expires Never Expires Never Expires Never Expires	No No No	No No
Users Users LDAP Certificate based Authentication Password Policy Account Suspension User Preferences User Preferences User Settings WLAN Integration User Stillings User Sti	nhadad dmazza shelsby aozimek dfields agreen chayes admin tmanning	Nicholas David Steve Adam Dan Andrew Chris	Hadad Mazza Helsby Ozimek Fields Green	//ADT //ADT //ADT //ADT //ADT	Never Expires Never Expires Never Expires	No	No
LDAP LDAP RADIUS RADIUS Certificate based Authentication Password Policy Account Suspension Suser Preferences Location Settings Locatio	dmazza shelsby aozimek dfields agreen chayes admin tmanning	David Steve Adam Dan Andrew Chris	Mazza Helsby Ozimek Fields Green	//ADT //ADT //ADT //ADT	Never Expires Never Expires	No	
RADIUS Image: Control of the set of	shelsby aozimek dfields agreen chayes admin tmanning	Steve Adam Dan Andrew Chris	Helsby Ozimek Fields Green	//ADT //ADT //ADT	Never Expires		No
KADUS Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authentication Image: Certificate based Authenticate based	aozimek dfields agreen chayes admin tmanning	Adam Dan Andrew Chris	Ozimek Fields Green	//ADT //ADT	Maximu Eveningen	No	No
Certificate based Authentication Password Policy Account Suspension User Preferences User Preferences User Settings Usy system Settings User WLAN Integration Certification	dfields agreen chayes admin tmanning	Dan Andrew Chris	Fields Green	//ADT	Never Expires	No	No
Password Policy 2 Account Suspension 2 User Preferences 2 Location Settings 2 System Settings 2 With Nintegration 2 With Statemation 2	agreen chayes admin triianning	Andrew Chris	Green		Never Expires	No	No
Account Suspension Let Preferences Let Preferences Let Vision Settings Let System Settings Let ViLAN Integration Let SM Integration	chayes admin trinanning	Chris		//ADT	Never Expires	No	No
User Preferences	admin tmanning		Hayes	//ADT	Never Expires	No	No
User Preterences Use Accation Settings User System Settings User Settings	tmanning	System	Superuser	//ADT	Never Expires	No	No
Image: Construction		Taber	Manning	//ADT	Never Expires	No	No
Image: System Settings Image: System Settings<	rnorth	Ray	North	//ADT	Never Expires	No	No
WLAN Integration	aellis	Adam	Ellis	//ADT	Never Expires	No	No
ESM Integration	kgispanski	Karen	Gispanski	//ADT	Never Expires	No.	No
a Maji con Integradon	twilcox	Todd	Wilcox	//ADT	Never Expires	No	No
22	mferrand	Michael	Ferrand	//ADT	Never Expires	No	No

Manage Users

Adding a User

Click Add to open the Add User Details dialog.

Jser Details					
Add user account	details. Select User Type	e: Local User 💌	1		1
		Local User	Lines Dala	Viewer	8
Login ID	-	LDAP User	User Kule	VICWCI	4
First Name		RADIUS User	Last Name		
Locations	//Locations;				Chan
User Properties	Password Settings				
Password			Confirm Password	d	
Email Address					
Session Timeout	💿 Session Neve	r Expires			
	🔿 Session Timed	out 10 min	s [10 - 120]		
Language prefere	nce English Only	*			
and the second second second second	Provide and a state of		1		

Adding User Details: User Properties Tab for Local User

Under **User Details**, select the user type (Local, LDAP, or Radius User). Superuser can create user accounts. For local authentication using password, it is necessary to create the user account using this screen before the user can log in. For a **Local User**, the superuser must specify the following fields:

- Login ID: Login ID of the user.
- **User Role:** This field specifies the role to be assigned to the user. The table below shows the user roles and their respective rights.
- First and Last Name: First and last name of the user.
- **Locations:** The list of locations where the user has access privilege consistent with the role.
- **Password**: Initial password of the user (which user can later change on his own).
- Confirm Password: Reenter the password to help confirm the password before saving.
- Email Address: Email address of the user.

For LDAP and RADIUS Users, creating user accounts using this screen is optional, because the user account gets automatically created (if not already present) upon the first successful login of the user who is authenticated via LDAP/RADIUS.

As a general rule, at the time of authenticating a user, the system always checks if the user password is locally available in the system. If it is not locally available, the system checks if the configuration is provided to access the LDAP authentication service. If so, the system attempts to verify the user password with the LDAP authentication service. If the user password is not available with the LDAP service, the system checks if the configuration is provided to access the RADIUS authentication service. If so, the system attempts to verify the user password with the RADIUS authentication service. If so, the system attempts to verify the user password with the RADIUS authentication service. In case of LDAP and RADIUS authentication, the system does not maintain local copy of the user password.

Jser Details Add user account	details. Select User Type: 🔟	AP User		1
Login ID		User Role	Viewer	1
First Name		Last Name		
Locations	//Locations;			Chan
User Properties	Password Settings			
Password		Confirm Passwor	d	
Email Address				
Session Timeout	💽 Session Never Expir	res		
	🔿 Session Timeout 📃	10 mins [10 - 120]		
Language prefere	ence English Only	~		
	CMT LOE(20) Acia/C	aloutta		

Adding User Details: User Properties Tab for LDAP User

For **LDAP User**, the superuser may create user accounts using this screen, prior to the first successful login of the user. For this, the following fields can be specified:

- Login ID: Login ID of the user.
- User Role: This field specifies the role to be assigned to the user. The table below shows the user roles and their respective rights.
- Locations: The list of locations where the user has access privilege consistent with the role.

Notes:

1. The User Role and Locations as specified above in the User Details screen are effective only if the corresponding attributes are not provided by the LDAP server at the time of authentication. When the LDAP server provides any of the above attributes, the LDAP provided values override the manually specified values in this screen.

2. To enable the LDAP authentication, configuration details to access the LDAP server must be provided in the LDAP configuration screen (described later). That screen also facilitates providing default User Role and Locations for all LDAP authenticated users, if the LDAP server does not provide those attributes. The User Role and Locations fields in the User Details screen facilitates providing specific default values for the corresponding attributes for the specific users, if the LDAP server does not provide them.

Jser Details Add user account o	details. Select User Type: 限	DIUS User 😽		
Login ID		User Role	Viewer 💉	1
First Name		Last Name		
Locations	//Locations;			Chan
User Properties	Password Settings			
Password		Confirm Password	d	
Email Address				
Session Timeout	Session Never Expi	res		
	🔘 Session Timeout	10 mins [10 - 120]		
Language preferer	nce English Only	V		
	(CMT +05:30) 0 dia/0	Calcutta		

Adding User Details: User Properties Tab for RADIUS User

For a **RADIUS User**, the superuser may create user accounts using this screen, prior to the first successful login of the user. For this, the following fields can be specified::

- Login ID: Login ID of the user.
- User Role: This field specifies the role to be assigned to the user. The table below shows the user roles and their respective rights.
- First and Last Name: First and last name of the user.
- Locations: This field specifies the locations where the user has access privilege consistent with the role.
- Email Address: This field specifies the email address of the user.

Notes:

1. The User Role and Locations as specified above in User Details screen are effective only if the corresponding attributes are not provided by the RADIUS server at the time of authentication. When the RADIUS server provides any of the above attributes, the RADIUS provided values override the manually specified values in this screen. The RADIUS server never provides First/Last Name and Email Address attributes.

2. To enable the RADIUS authentication, configuration details to access the RADIUS server must be provided in the RADIUS configuration screen (described later). That screen also facilitates providing default User Role and Location values for all RADIUS authenticated users, if the RADIUS server does not provide those attributes. The User Role and Locations fields in the User Details screen facilitates providing specific default values for the corresponding attributes for the specific users, if the RADIUS server does not provide them.

The Session Timeout, Language and Time Zone settings are applicable to all types of users.

- **Session Timeout:** Specify the time after which the user will be logged out automatically if the system does not detect any activity.
- Session Never Expires: Select this check box if you do not want the session to expire in response to inactivity.

• Session Timeout: Specify the number of minutes after which the system automatically logs out the currently logged in user when there is no activity on the Console for the Session Timeout period

(Minimum: 10 minutes; Maximum: 120 minutes)

- Language Preference: Select English or Multilingual support from the drop-down list.
- **Time Zone:** Select the appropriate time zone for the user

The following table summarizes the rights for various user roles.

Table 5 User Roles and User Rights

Operations	User Roles				
	Superuser	Administrator	Operator	Viewer	
User account management					
Set or modify identification and authentication option (Password only, Certificate only, Certificate and Password, Certificate or Password)	Yes	No	No	No	
Add and delete users	Yes	No	No	No	
View and modify properties of any user (User Management screens)	Yes	No	No	No	
Define password strength, account locking policy, maximum concurrent sessions for all users	Yes	No	No	No	
View and modify User Preferences (email, password, session timeout)	Yes (self only)	Yes (self onlv)	Yes (self onlv)	Yes (self onlv)	
User actions audit					
Download user actions audit log	Yes	No	No	No	
Modify user actions audit lifetime	Yes	No	No	No	
System settings and operating policies					
Modify system settings and operating policies (all settings under Administration tab other than User Management, Logs, Login configuration)	Yes	Yes	No	No	
Events, devices and locations					
View generated events	Yes	Yes	Yes	Yes	
Modify and delete generated events	Yes	Yes	Yes	No	
View devices	Yes	Yes	Yes	Yes	
Add, delete, and modify devices (APs, Clients, Sensors)	Yes	Yes	Yes	No	
View locations	Yes	Yes	Yes	Yes	
Add, delete, and modify locations	Yes	Yes	Yes	No	
Calibrate location tracking	Yes	Yes	Yes	No	
Reports					
Add, delete, modify Shared Report	Yes (all)	Yes (only self created)	Yes (only self created)	No	
Generate Shared Report	Yes	Yes	Yes	Yes	
Schedule Shared Report	Yes	Yes	Yes	No	
Add, delete, modify, generate, schedule My Report	Yes (only self created)	Yes (only self created)	Yes (only self created)	No	

Note:

1. There can be as many Superusers as required. Superuser always has rights to root of the location tree.

2. *The role is unique for any user.*

The **Password Settings** tab applies to only locally authenticated users. It does not apply to LDAP or RADIUS authenticated users. The Password Settings menu has the following fields:

ogin ID		User Role	Viewer 💉	1
irst Name		Last Name		
ocations	//Locations;			Chan
Password Exp	iry Duration 60 🗘 days [1 - 365]	Password Expiry	Warning 15 💲 days [1 - 60]	
Expiry Date	Password never expires			

Adding User Details: Password Settings Tab

- **Password never expires:** If selected, the password does not expire over time. If this option is selected, the fields, **Password Expiry Duration**, **Password Expiry Warning**, and **Expiry Date** are disabled.
- **Password Expiry Details:**If selected, specify the following parameters:
- Password Expiry Duration: Enables you to specify the duration for which the specified password is valid. If the Password Expiry Duration is less than 15 days, the system raises a Password Expiry Warning message every time the user logs into the Console

(Minimum: 1 day; Maximum: 365 days)

- **Expiry Date:** Shows the password expiry date and time
- Password Expiry Warning: Enables you to specify the number of days before the password expiry date that
 a password expiry warning should appear. The warning appears every day until you change the password.
 Once you change the password, the system updates the Expiry Date depending on the value specified in the
 Password Expiry Duration field

(Minimum: 1 day; Maximum: 60 days)

Note: For the LDAP and RADIUS users, the Password Settings tab is inactivated.

Click Add to add the details for a new local user.

Editing a User

To edit the details of an existing user,	double-click a row	or select a row	and click Edit to	open the Edit User	Details
dialog.					

Jser Details				
User Type:	Local User			
Login ID	mferrand	User Role	Viewer 🖌	1
First Name	Michael	Last Name	Ferrand	
Locations	//ADT;			Chan
User Properties	Password Settings			
Email Address Session Timeout	mferrand@adt.com Session Never Expires Session Timeout	mins [10 - 120]		
Language preferen	ce English Only	2		
Time Zone	(GMT -05:00) America/Ne	w_York 🏾 😽		
Jser account account account suspend	essibility ed			

Editing User Details

The Edit User Details dialog is similar to the Add User Details dialog.

Any field value, other than Login ID, that has been specified manually while adding user details, can be modified at the time of editing the user details.

Under User Account Accessibility, the superuser can do the following for other users.

- Account suspended: Enable a user account that has been temporarily suspended due to failed login attempts. If the user account has been disabled due to failed login attempts then the Account suspended check box is enabled. The administrator can enable the user account by un-checking the Account suspended check box.
- Enable/disable a user account permanently.

Click **Save** to save all the changes.

Note: A dark highlight for an entry in the user list indicates that the user account is disabled or suspended *permanently*.

Deleting a User

Select a row and click **Delete** to delete specific user account from the system.

For LDAP and RADIUS authenticated users, it is necessary to delete user account from the system in addition to deleting it from the LDAP/RADIUS server. Else, email notifications will continue to be sent to the user even after the account is deleted from LDAP/RADIUS server.

LDAP Server Configuration

The system can use an LDAP server for user authentication. The LDAP Configuration screen facilitates configuration of the LDAP server access parameters.

LDAP Configuration Provide configuration details to access the entryprise LDAP Server to facilitate LDAP authentication for users. Provide configuration details to access the entryprise LDAP Server to facilitate LDAP authentication for users. Provide configuration details Provide configuration details Connection Stuppendic Descrue Stuppendic Descrue Stuppendic Descrue Stuppendic Default Provides of DAP Users User Nonaccion Details Descrue Stuppendic Default Provides of DAP Users User Role User	Global 🗊 Local	Advanced - LDAP Configuration	on	
Conta texturgs Conta texturgs Conta texturgs Conta texturgs Conta texturgs Contaction betails Contaction betails Parse Hamsgement Contaction betails Password Policy Varia User Straturgs Sociations Statungs Sociations Statungs <th></th> <th>LDAP Configuration</th> <th></th> <th></th>		LDAP Configuration		
Image: Spectro Goard SAFE Image: Spectro Goard SAFE <th>🗭 Global Policies</th> <th>Provide configuration details to access the e</th> <th>nterprise LDAP Server to facilitate LDAP</th> <th>authentication for users.</th>	🗭 Global Policies	Provide configuration details to access the e	nterprise LDAP Server to facilitate LDAP	authentication for users.
IDAP Integration Details IDAP Integration Details IDAP Integration Details Primary Server IP Address/Hosthame Backup Server IP Address/Hosthame IP Server IP Address/Hosthame	E Went Settings	Enable LDAP		
Connection Details Primary Server Port Backup Server Port Backup Server Port Backup Server Port Backup Server Port Constitution Details Vertry LDAP Configuration Details Base Distinguished Name (DN) User Role Vertry LDAP Server Societ DAP Configuration Details Base Distinguished Name (DN) User Role attribute Constitutions User Role attribute DAP Configuration Details Base Distinguished Name (DN) User Role attribute User Role attribute User Role attribute User Role Werener Authentication required to search LDAP Admin User DN Password Base Distry Password Base Name Password Base Name Password Base Name Password	Device Settings	LDAP Integration Details		
Vesrs Primary Server IP Address/Hostname Pacups Primary Server IP Address/Hostname RADUS Backup Server PC Certificate based Authentication Backup Server Pot Password Policy Backup Server Pot Vesr Preferences User Preferences Load Description Dare Dolfgueithed Name (DN) Vesr Potingueithed Name (DN) Description Vesr Potingueithed Name Description Vesr Potingueithed Name Description Vesr Potingueithed Name <td< td=""><td>User Management</td><td>Connection Details</td><td></td><td></td></td<>	User Management	Connection Details		
Primary Server Port 380 RADUS Backup Server Port Backup Server Port 380 Backup Server Port 380 Password Policy Backup Server Port Password Policy Enforce Use of SILTLS User Preferences Enforce Use of SILTLS Wick's Integration User Potences Wick's Integration User Role User Role User Role User Role User Role User Role User Role User Role Change LDAP Authentication Petals Backup Server ID ALTIPUT User Role User Role User Role User Role User Role User Role User Authentication Petals User Role User Role User Role User Role User Role User Role User Settings User Name Password Password Password	Users	Primary Server IP Address/Hostname		
RADUS Backup Server IP Address/Hostname Backup Server Port Backup Server Fort Backup Server Sertificate User Preferences Location Settings System Settings User Preferences User Preferences User Relie User Relie User Relie Verify LDAP Server's Certificate CA Cartificate Management DAP Configuration Details Base Distinguished Name (DN) Configuration Details Base Distinguished Name (DN) Configuration Details User Relie User Relie Verify LDAP Server's Certificate Configuration Details User Relie User Relie Verify LDAP Server's Certificate Configuration Details User Relie User Relie Verify LDAP Server's Certificate Configuration Details User Relie Verify LDAP Server's Certificate Verify LDAP Server's Certificate Configuration Details User Relie Verify LDAP Server's Certificate Verify LDAP Server's Certificate Change Verify LDAP Authentication required to search LDAP Admin User DN Password Verify LDAP Server's Certificate Verify LDAP	- 🖗 LDAP	Primary Server Port	389	-
Backup Server Port Password Policy Account Supposion User Preferences User Preferences WIAN Integration User Role Attribute User Role Attribute User Role Attribute User Role Password Password	RADIUS	Backup Server IP Address/Hostname		
Password Policy Account Suspension User Preferences System Settings System Settings Base Distinguished Name (DN) IsoP Integration User Profesences User ID Attribute IsoP Integration User Role Attribute Default Privileges for LDAP Users User Role User Role Verify IDAP Autientication Details Content of the second Dape Admin User DN Password Change IDAP Autientication Details Content of the second Dape Admin User Note Password Test Settings Wiser Role User Role User Role Verify IDAP Autientication Details IDAP Autientication Details User Role Verify IDAP Users User Role User Role Verify Appendiates DN Password Test Settings User Role Verify Appendiation Passe DN Password Test Settings	Certificate based Authentication	Backup Server Port		
Account Suspension User Preferences LDAP Configuration Details Base Distinguished Name (DN) WILAN Integration User ID Attribute User Role Verwar Integration User Role Verwar Locations Locations Locations Locations Location Attribute Default Privileges for LDAP Users User Role Vermine To N Admin User DN Password Test Settinge	Password Policy	Enforce Use of SSL/TLS		
User Preferences Location Settings System Sattings WLAN Integration User ID Attribute Default Privileges for LDAP Users User Role Verwar Locations LDAP Authentication Petals Locations Authentication Petals Locations Locations Locations LDAP Authentication Petals Locations Locations <td>Account Suspension</td> <td>Verify LDAP Server's Certificate</td> <td>CA Certificate Management</td> <td></td>	Account Suspension	Verify LDAP Server's Certificate	CA Certificate Management	
LDAP Configuration Details System Settings WIAN Integration WIAN Integration User ID Attribute User Role Attribute User Role Attribute User Role Attribute User Role Vewer Locations //ADT Change LDAP Authentication Petails User ID Attribute User Role Vewer Locations //ADT Change LDAP Authentication Petails User Name User Name Password	Ser Preferences			
System Settings WLAN Integration User ID Attribute ID SpectraGuard SAFE Default Privileges for LDAP Users User Role Vewer LDAP Authentication Details Authentication required to search LDAP Admin User DN Password Test Settings	Cocation Settings	LDAP Configuration Details		
WLAN Integration User Role Attribute SpectraGuard SAFE User Location Attribute Filter String Default Privileges for LDAP Users User Role User Role Locations //ADT Change Location required to search LDAP Admin User DN Password Test Settings User Name Password	😢 System Settings	Base Distinguished Name (DN)		
ESH Integration User Role Attribute Integration SAFE User Location Attribute Filter String Default Privileges for LDAP Users User Role Vewer Locations Locations Location required to search LDAP Admin User DN Password Test Settings User Name Password	WLAN Integration	User ID Attribute	cn	
SpectraGuard SAFE User Location Attribute Filter String Default Privileges for LDAP Users User Role User Role Locations Locations LDAP Authentication Details Admin User DN Password Test Settings User Name Password Test Settings	ESM Integration	User Role Attribute		
Filter String Default Privileges for LDAP Users User Role User Role Locations //A01 Change LDAP Authentication Details Authentication required to search LDAP Admin User DN Password Test Settings User Name Password Test	10 Spectra Guard SAFE	User Location Attribute		
Default Privileges for LDAP Users User Role User Role Uccations //AOT Change LDAP Authentication Details Authentication required to search LDAP Admin User DN Password Test Settings User Name Password Test		Filter String		
User Role Vewer Locations //ADT Change LDAP Authentication Details Authentication required to search LDAP Admin User DN Password Test Settings User Name Password Test		Default Privileges for LDAP Users		
Locations //ACT Change LDAP Authentication Details Authentication required to search LDAP Admin User DN Password Test Settings User Name Password Test)		User Role	Viewer	1
LDAP Authentication Details Admin User DN Password User Name Password Test		Locations	//ADT	Change
Authentication required to search LDAP Admin User DN Password Test Settings User Name Password Test		LDAP Authentication Details		
Admin User DN Password User Name Password Test		Authentication required to search LD	DAP	
Password Test Settings User Name Password Test		Admin User DN		Append Base DN
Test Settings User Name Password Test		Password		
User Name Password Test		Test Settings		
Password Test		User Name		
		Password		Test
It may take upto five minutes to test these settings.		It may take upto five minutes to test the	se settings.	

LDAP Configuration

Check Enable LDAP to enable user authentication using an LDAP compliant directory.

LDAP Integration Details: Provide configuration parameters for the system to be able to access the LDAP compliant directory. Following details can be provided using this screen.

- **Connection Details:** Provide details for the system to be able to establish connection with the LDAP server.
 - Primary Server IP Address/Hostname: Specifies the primary server IP address/Hostname of the LDAP server.
 - Primary Server Port: Specifies the primary server port number of the LDAP server. (Default: 389)
 - Backup Server IP Address/Hostname: Specifies the backup server IP address/Hostname of the LDAP server.
 - Backup Server Port: Specifies the backup server port number of the LDAP server.
 - Enforce Use of SSL/TLS: When this option is checked, only the SSL/TLS connection to the LDAP server is allowed. When it is not checked, either of the Open or SSL/TLS connection to the LDAP server is allowed.
 - Verify LDAP Server's Certificate: When this option is checked, the connection to the LDAP server
 is not allowed unless the certificate check passes. Click Certificate Management to add trusted root
 CA Certificate(s) for the LDAP server. When this option is not checked, the connection to the LDAP
 server is allowed without checking the LDAP server certificate.
 - **LDAP Configuration Details:** Provide details for the system to be able to search records in the LDAP server.

Base Distinguished Name: Specifies the base distinguished name of the directory to which you
want to connect, for example, o=democorp, c=au.

Note: Distinguished Name is a unique identifier of an entry in the Directory Information Tree (DIT). The name is the concatenation of Relative Distinguished Names (RDNs) from the top of the DIT down to the entry in question.

• User ID Attribute: Specifies the user ID attribute string that the system uses to identify the user, as defined in your LDAP schema.

(Default: cn)

- User Role Attribute: Specifies the user role attribute string that the system uses to identify the user's role, as defined in your LDAP schema.
- User Location Attribute: Specifies the user location attribute string that the system uses to identify the locations where the user is allowed access, as defined in your LDAP schema.
- **Filter String**: Specifies certain attributes: existing or new: that you can use for different users, based on which the server filters the users, for example, (IsUser=A). This feature can help restrict the use of the system to a certain set of users.
- **Default Privileges for LDAP Users:** This section specifies the default role and the default locations assigned when new LDAP users log in, for the case where the role and locations attributes are not provided by the LDAP server. Note that the default values here apply to all users authenticated via LDAP. Specific default values can also be provided for the specific LDAP users using **Edit User** dialog. If the LDAP server provides user role and locations attribute at the time of authentication, the attributes provided by the LDAP server will override the default role and locations attributes.
 - **User Role**: Enables you to specify the default role for the new LDAP users. You can select one of the following four options. The default user role is *Viewer*.
 - 1. Superuser
 - 2. Administrator
 - 3. Operator
 - 4. Viewer
 - •
 - **Locations**: Displays the list of locations to which a new LDAP user has access rights.
 - Click Change... to open the Assign Locations dialog. Here, you can view the complete list of locations and select the locations to which the LDAP user can have access rights. Click OK to assign the selected location(s) to the user.
- **LDAP Authentication Details:** Specify user credentials required to search the LDAP compliant directory. This is required only in case the directory does not allow anonymous search.
 - Select Authentication Required to search LDAP? if the LDAP server requires administrator login to search the LDAP compliant directory. Specify the Admin User DN and Password to log in.
 - If you select Append Base DN, the Base Distinguished Name specified in LDAP Configuration Details is appended to the Admin User DN.
- **Test Settings:** Enables you to test whether the specified settings are correct. To verify the settings, enter the **User Name** and **Password** for a specific user and click **<Test>**.

Note: Test is not available unless you change the settings. Apply is unavailable until you use Test.

RADIUS Server Configuration

The system can use a RADIUS server to facilitate user authentication. The RADIUS Configuration screen facilitates configuration of the RADIUS server access parameters.

Ciobal Cocci Cocci Ciobal Cicco Cicc	Juanced - RADIUS J9 Configuration creen allows configuration ate control over Commu- tive checkboxes for CLI le RADIUS Authentication hentication Server D hentication Server D imary P Address/ Hostname ort Number hared Secret	Configuration Infor RADIUS server authentic Interface (CLI) and Gra and GUI login below. In Advanced Settings etails Interface Interfac	tion. Use the checkbox below to phical User interface (GUI) Login Secondary IP Address/ Hostname Port Number Shared Secret	enable / disable RADIUS authentic can be achieved by using the 1812	cation.
Clobal Policies RADIU Clobal Policies Separ Clobal Policies Separ Clobal Policies France Clobal Policies Enab Certificate based Authentication Pri Password Policy S Account Suspension S User Preferences Enal Matter Location Settings Closidio Settings Enal	JS Configuration creen allows configuration ate control over Comma tive checkboxes for CLI le RAD/US Authentication hentication Server D imary P Address/ Hostname ort Number hared Secret	n for RADIUS server authentica nd Line Interface (CLI) and Gra and GUI login below. n Value of the settings and Advanced Settings tails	tion. Use the checkbox below to phical User interface (GUI) Login Secondary IP Address/ Hostname Port Number Shared Secret	enable / disable RADIUS authentic can be achieved by using the 1812	cation.
Clobal Policies This is separative settings With Event Settings Enable	creen allows configuration tet control over Comma titve checkboxes for CLI le RADIUS Authentication hentication Account thentication Server D imary P Address/ Hostname ort Number hared Secret	n for RADIUS server authentics and GUI login below. n v and GUI login below. n v and GUI login below. atails 1812	tion. Use the checkbox below to phical User interface (GUI) Login Secondary IP Address/ Hostname Port Number Shared Secret	enable / disable RADIUS authentic can be achieved by using the 1812	cation.
Werent Settings Doponic respective Will Device Settings Enable Wilser Management Autility Wilser's Autility Wilser's Autility Wilser's Autility Print RADIUS Certificate based Authentication Print Password Policy S Wilser Preferences Enable Wilser Preferences Enable Wilser Settings Enable	Le Condo Vor Condo Le RADIUS Authentication hentication Account hentication Server D Imary Address/ Hostname ort Number hared Secret	n and GUI login below. n via Advanced Settings stails 1812 Test	Secondary IP Address/ Hostname Port Number Shared Secret	1812	
Image: Settings Enable Image: User's Authors Image: User's Image: User's	le RADIUS Authentication hentication Account hentication Server D imary P Address/ Hostname ort Number harad Secret	n V ing Advanced Settings tails 1812 Test	Secondary. IP Address/ Hostname Port Number Shared Secret	1812	
User Management Aut Users Aut LDAP Pri Cartificate based Authentication Pri Password Policy S Account Suspension S Location Settings Enal System Settings Enal	hentication Account thentication Server D imary P Address/ Hostname ort Number thared Secret	Ing Advanced Settings	Secondary IP Address/ Hostname Port Number Shared Secret	1812	
Loap Loap Loap Loap Loap RADIUS RADIUS Reading Authentication P Password Policy S S Loacount Suspension Loacount Suspension Loacount Suspension Loacount Suspension Section Settings Section Settings	hentication Account hentication Server D imary P Address/ Hostname ort Number hared Secret	Advanced Settings etails	Secondary IP Address/ Hostname Port Number Shared Secret	1812	
LDAP LDAP RADIUS RADIUS Password Policy Account Suspension User Preferences Location Settings System Settings System Settings	hentication Server D imary P Address/ Hostname ort Number ihared Secret	1812	Secondary IP Address/ Hostname Port Number Shared Secret	1812	
Provide Provide Password Policy S Account Suspension S User Preferences Enal Location Settings Enal System Settings Enal	mary P Address/ Hostname ort Number hared Secret	1812	IP Address/ Hostname Port Number Shared Secret	1812	
Image: Addition Image: Addition	r Maaress/ Hosthame ort Number hared Secret	1812	Port Number Shared Secret	1812	
Certificate based Authentication Password Policy Society Account Suspension Location Settings System Settings Enal	ort Number hared Secret	Test	Shared Secret	1812	
Password Policy Account Suspension User Preferences Location Settings System Settings Enal	hared Secret	Test	Shared Secret		
User Preferences Location Settings Ena System Settings Ena		Test			
User Preferences Enal				Test	
Location Settings	hie RADIUS Server Inte	aration for CLT login			
🛍 System Settings Enal		and the car to but I			
	ble RADIUS Server Inte	gration for GUI login 🗌			
WLAN Integration	dor Specific Attribut	es (Default Values)			
Use Use	the following default val	ues when vendor specific attribu	ites are not defined for RADIUS u	iser.	
All All	low-CLI-Access	No			
Al	low-GUI-Access	No			
GU	JI-Role	Wawer			
GU	JI-Allowed-Location	MADT/URKROWN	Change		

RADIUS Configuration

Check Enable RADIUS Integration for CLI login to enable CLI user authentication using RADIUS and check **Enable RADIUS Integration for GUI login** to enable GUI user authentication using RADIUS.

The RADIUS Configuration screen has Authentication, Accounting, and Advanced Settings tabs.

- The Authentication tab is used to specify configuration to access the RADIUS Authentication server
- The Accounting tab is used to specify configuration to access the RADIUS Accounting server

• The **Advanced Settings** tab is used to specify the realm (domain) for the CLI and the GUI users. You can also

specify in this tab how the real name is to be appended to the username (prefix notation or postfix notation).

User Authentication

The systems supports four authentication options. The superuser has to set any one authentication option, and it then applies to all users. The four authentication options supported by the system are as follows:

1. **Password only**: In this option, the user authentication is performed using the password. The user has to enter the username and the password at the login prompt. The password may be locally verified by the system or may be verified using the external LDAP or RADIUS authentication service, as appropriate. When this authentication option is set, the login screen appears as follows:



Login Screen - Password only authentication

2. Certificate only: In this option, the user authentication is performed using the client certificate (such as smart card). The user has to insert a smart card containing the client certificate in a reader attached to the computer from where the console is accessed and then press the Login button. The system then verifies the client certificate and obtains user identity (username) from the certificate. Other attributes for the user are retrieved either locally or from the external authentication services such as LDAP or RADIUS, as appropriate. When this authentication option is set, the login screen appears as follows:



Login Screen - Certificate only authentication

3. **Certificate and Password**: In this option, both the client certificate and the password are required for the user authentication. The user has to insert a smart card containing the client certificate in a reader attached to the computer from where the console is accessed, as well as enter the password at the login prompt. The system verifies the password locally or using the external LDAP or RADIUS authentication service, as appropriate. When this authentication option is set, the login screen appears as follows:



Login Screen - Certificate and Password authentication

4. **Certificate or Password**: In this option, the user authentication is permitted either using the password or using the client certificate. This option is appropriate for organizations which have only partially migrated to using smart cards for authentication. At login prompt, the user can select certificate authentication by checking the **Use certificate for login** box or continue with password authentication by enterping login name and password. When this authentication option is set, the login screen appears as follows:



Login Screen - Certificate or Password authentication

The superuser can use following screen to set one of the above four authentication options namely *Password only*, *Certificate only*, *Certificate and password* or *Certificate or password*.

📰 Dashboard 💇 Events 🎼 Devices 🌰	Locations 📴 Reports 🔍 Forensics 🌉 Administration	Jun 13 2011, 11:49:27 AM (GMT +0530) 🔃 💽 💽 🐱
😰 Global 😰 Local	🗊 Certificate based Authentication	
	Certificate based Authentication	
Cobal Policies Cobal Policies Cobal Policies Comment C	The system can be configuration of certificate users using digital certificates. This screen allows the configuration of certificate based authentication. Enable certificate based authentication Use field in certificate as user identity Allow access without certificate Users must provide password along with certificate Certificate Revocation Certificate Revocation Check certificate revocation Lists (automatically downloaded) Treat certificate as vield when certificate status cannot be confirmed Restore Defaults	

Certificate Authentication

The required authentication option can be activated based on the various combinations of the **Enable certificate based authentication** box, **Allow access without certificate** box, and **Users must provide password along with certificate** box.

The following table describes the activation of the authentication options based on the check boxes selected by the user.

Authentication option to activate	Check box to be selected				
	Enable certificate based authentication	Allow access without certificate	Users must provide oassword along with certificate		
Password only	No	-	-		
Certificate only	Yes	No	No		
Certificate and password	Yes	No	Yes		
Certificate or password	Yes	Yes	No		

Note: In order to use certificate based authentication, it is necessary that the GUI host is able to access the server at TCP port 4433. If there is a firewall between the GUI host and the server, port 4433 must be opened from the host to the server, in order to be able to use certificate based authentication.

When either *Certificate only, Certificate and Password,* or *Certificate or Password* option is activated, the additional details should be provided as follows:

- The field in the client certificate from which user identity can be retrieved by the system.
- Root CA certificates to facilitate the verification of the client certificate.
- Preferred method to check for certificate revocation.

Password Policy

The Password Policy determines the minimum requirements for system passwords. This policy applies to all User Roles: superuser,, administrator, operator, and viewer. If you change this policy, older passwords are not affected. Only passwords created after a policy change are subject to the new policy. This setting applies only to local authentication and does not apply to LDAP and RADIUS authentication.



Password Policy

Under **Password Policy**, you can specify the following:

• **Minimum number of characters:** Enables you to specify the minimum number of characters to be used for constructing passwords.

(Minimum: 4; Maximum: 15; Default: 6)

• Numeric Characters required?: Enables you to enforce the use of numeric characters for constructing passwords.

(Default: No)

• **Special Characters required?:** Enables you to enforce the use of special characters for constructing passwords.

(Default: No)

Account locking

Account locking allows the superuser to specify the account locking policy for the selected user type – Superuser, administrator, operator, or viewer. Account locking protects the system from spurious logins through dictionary attacks. This setting applies only to those authentication options which use password as at least one of the authentication mechanisms.

📰 Dashboard 👷 Events 🔯 Devices 🍖 Loca	ations 🗄 Reports 🔍 Forensics 🖉 Admi	nistration	Oct 12 2011, 06:39:48 AM (GMT -0400) 🔯 🕐 든 👰 📆
🛱 Global 🗊 Local	🛞 Account Suspension		
Cabindard C events C	Account Suspension Select User Role Supervise Account Suspension Policy for Role Define the account suspension Policy for Role Define the account suspension policy for Role Account Suspension Policy for Role Suspension Time Apply Cancel	<pre>statute statute statute statute d be enforced.</pre>	UCt 12 2011, UG:39:48 AY (GYT -9400) 🕐 🖉 🗲

Account Suspension

Under Account Suspension, you can select the User Type and then specify the following:

• Allowed Number of Login Failures: Enables the superuser to configure the number of failed login attempts after which the account is suspended.

(Minimum: 3 times in 5 minutes; Maximum: 10 times in 30 minutes; Default: 3 times in 10 minutes)

• **Suspension Time:** Enables the superuser to define the amount of time for which the selected user is prevented from accessing the system.

(Minimum: 5 minutes; Maximum: 30 minutes; Default: 15 minutes)

User Preferences

The User Preferences screen enables a user to change his/her own login password and other preferences.

Dashboard 💇 Events 💊 Devices 🏠 Lo	cations 📑 Reports 🔊 Fore	nsics M Administration	Oct 16 2011, 12:38:18 AM (GMT -0400) 😰 💽 💽
🛱 Global 🛱 Local	🕒 User Preference	es	
	Password Details		
Clobal Policies	You can change your pa Login ID	assword or notification email address on this screen. admin	
Device Settings	Email Address*	network@adt.com	
User Management	all available		
🛃 Users	New Pacsword		
- dap	Confirm Password		
RADIUS	User Preferences		
- 📔 Certificate based Authentication	You can change your se Session Timeout	ssion timeout interval, language settings or time zone on this screen. ③ Session Never Expires ○ Session Timeout 10 mins [10 - 120]	
- 🛞 Account Suspension	Language preference	English Only	
Ser Preferences	Time Zone	(GMT -05:00) America/New_York	
ESM Integration			

User Preferences

Under **Password Details**, user can specify/modify his email address and password. Password change from this screen is not applicable for the users using LDAP/RADIUS authentication, or for users for whom password based authentication has been disabled. Also, changing the email address from this screen is not applicable for LDAP authenticated user.

Under **User Preferences**, the user can change his/her own Session Timeout, Language Preference, or Time Zone. Click **Apply** to save to the new settings.

Location Settings

The Location Settings dialog sets the following location settings in the system.

Auto Location Tagging

A location tag that is attached to a device or an event helps identify the location of that event or device. The system has an Auto Location Tagging feature, which refers to the capability of the system to automatically 'tag' the devices and events to the locations where they have been detected.

The **Auto Location Tagging** screen enables you to configure the settings for automatic tagging of devices discovered by the system and events generated by the system.

📰 Dashboard 👷 Events 🖕 Devices 🏫	Locations 🖹 Reports 🔍 Forensics 🖉 Administration 💕 Jun 13 2011, 12	2:02:27 PM (GMT +0530) 🕼 🕐 📘) 🛛 🗄
🛱 Global 🕅 Local	Advanced - Auto Location Tagging Configuration		
Clobal Policies Clobal Polici	Aute Location Tagging Configuration Choose the settings for auto location tagging. This feature allows new devices or events to be automatically tagged with a location. Devices Appendix and the settings for auto location tagging for that device, you must delete the device and let it be re-discovered. Sensors can only be tagged manually. Choose location tag of the Sensor that sees the highest RSSI value for that device. Ochoose location tag of the Sensor that sees the highest RSSI value for that device. Discard Sensors that see RSSI that is Is Is and on the location of the device. Devices Revents Revents Choose location tag of the Sensor that sees the highest RSSI value for that device Discard Sensors that see RSSI that is Is Is and the primary device (AP, Client or SpectraGuard Enterprise identifies a primary device (AP, Client or SpectraGuard Sensor) for each event. Auto location tagging of events is done based on the tag for the primery device (AP, Client or SpectraGuard Sensor) for each event. Auto location tagging of events is done based on the tag for the primary device (AP, Client or SpectraGuard Sensor) Is never re-tagged. You can tag the location of an event manually by right clicking on it and selecting "Change location". Isotory Cancel Reverse Defaults		

Auto Location Tagging

Auto Location Tagging Configuration contains the following options:

- **Devices:** Based on the initial location of the device, the APs and Clients are auto-tagged immediately upon discovery. You can select how the system should compute the initial location tag of the APs or Clients. The system never auto-tags an AP or Client, if it is tagged manually. To re-enable auto location-tagging for a device, you must delete the device and let the system re-discover it. You must manually tag sensors. You can do one of the following:
- Choose the location tag of the sensor that sees the highest RSSI value for that device.
- Choose the location tag of the selected number of sensors that see the highest RSSI values for that device. (Minimum: 2; Maximum: 10; Default: 2)

You can also discard the sensors that see a lower RSSI after comparing the value with a sensor that reports a higher RSSI.

(Minimum: 20 dB; Maximum: 40 dB; Default: 30 dB)

Events: The system tags events based on the location of the devices that participate in the events. The system
initially identifies a primary device — AP, Client, or Sensor for each event. The system automatically tags the
location of events based on the tag for the primary device associated with the event.

Note: The system never retags an event. You can tag the location of an event manually on the *Events* screen by right-clicking the event and from the resulting menu by selecting *Change Location*.

Location Tracking

The location of a particular device can be tracked using the location tracking feature. The system needs at least three sensors to perform location tracking. The **Location Tracking** screen enables you to define the parameters that control location tracking.

📰 Dashboard 💇 Events 👹 Devices 🌰	Locations 🖹 Reports 🔊 Forensics 🌆 Administration		Jun 13 2011, 12:10:30 PM (GMT +0530) 📝 🕐 든 🧔 🔣
🛱 Global 🗊 Local	📧 Advanced - Default Location Tracking Parar	neters	
	Default Location Tracking Parameters		
Boo	Define the parameters to control location tracking.	Constrained Likelihand	
Device Settings	Manimum and the second to use for Landian Tradice		24 July 24 Jul
	Patente Targer in Sensors to use for Location Tracking	4 *	
lasstion Sattings	Derault Transmit Power of AP (mw)	30 -	
Auto Location Traging	Default Transmit Power of Client (mw)	10 👽	
Location Tracking			
Live RF Views	Apply Cancel Restore Defaults		
RF Propagation			
• Le System Settings			
WLAN Integration			
ESM Integration			
🗄 🏠 SpectraGuard SAFE			

Location Tracking

Default Location Tracking Parameters contains the following options:

- **Location Tracking Technique:** Select the technique used for location tracking. The technique available is *Generalized Likelihood*.
- Maximum number of Sensors to use for Location Tracking: Select the maximum number of sensors used for location tracking. Sensors track down the location of a device and the system uses sensors that see the maximum values. A higher value is likely to give better results.

(Minimum: 3; Maximum: 10; Default: 4)

• **Default Transmit Power of AP (mW):** Location tracking needs as input the transmit power of the AP being located. When transmit power is unknown, the default value set here is used.

(Minimum: 1 mW/0 dBm; Maximum: 100 mW/20 dBm; Default: 30 mW/15 dBm)

• **Default Transmit Power of Client (mW):** Location tracking needs as input the transmit power of the Client being located. When transmit power is unknown, the default value set here is used.

(Minimum: 1 mW/0 dBm; Maximum: 100 mW/20 dBm; Default: 10 mW/ dBm)

• Signal Strength Monitoring Devices: Location tracking is based on the signal strength of the monitoring devices. This value can deviate from the actual values because of subtle variations in the RF environment. You can specify APs only, Sensors only, and Sensors and/or APs to be used to control location tracking. Using the system's Application Programming Interface (API), APs can be reported as a source of signal strength. Information from these APs can be used for location tracking.

Live RF Views

The Live RF Views screen enables you to define the parameters that are used in live RF views. These parameters are
specific to each environment. Tuning the parameters enables you to see more accurate views.

Dashboard 💇 Events 🔯 Devices 🐔	Locations Reports Forensics Administration		Jun 13 2011, 12:12:27 PM (GMT +	0530) 😫 🕐 🔚 🧕
🛱 Global 🗱 Local	🔍 🔍 Advanced - Default Live RF View Pa	arameters		
	Default Live RF ¥iew Parameters			
Global Policies	Define the default narameters to display Live DF Vie	awo. These parameters typically	are specific to each environment	
10 Event Settings	Tuning the parameters enable you to see more acc	urate views.	are specific to each environment.	
Device Settings	Intrusion Detection and Prevention Regions		The second second	
🔯 User Management	RF view display.	is the RSSI value at which to cu	on the Detection Range	
🏠 Location Settings	The 'Intrusion Prevention Display Threshold' contru	ols the RSSI value at which to r	t off the 'Prevention Range'	
Auto Location Tagging	RF view display.			
Location Tracking	Besides, both Detection and Prevention ranges are	e affected by various parameter	in 'Default RF Propagation	
Live RF Views	Settings' of the Administration Tab.			
RF Propagation	The reliability of the prevention also depends on th	ne 'Intrusion Prevention Level',	hich can be set at the	
System Settings	Local Policies->Operating Policies->Intrusion Previ	ention node of the Administratio	t lab.	
WLAN Integration	Intrusion Detection Display Inreshold (dBm)	-85		
Corry ESM Integration	Intrusion Prevention Display Threshold (dBm)	-75		
SpectraGuard SAFE				

Live RF Views

Default Live RF Views Parameters contains the following options:

- **Intrusion Detection and Prevention Regions:** Specify the dBm values for which the system shows the intrusion detection and prevention regions in the sensor coverage views.
- Intrusion Detection Display Threshold (dBm): Detection Range is the area over which sensors can reliably detect wireless activity. Intrusion Detection Display Threshold determines the threshold for this range. (*Default: -85 dBm*).
- Intrusion Prevention Display Threshold (dBm): Prevention Range is the area over which sensors can
 prevent unauthorized wireless activity. Intrusion Prevention Display Threshold determines the threshold
 for this range. (Default: -75 dBm)

Both the Detection and Prevention ranges are affected by parameters in the RF Propagation section.

Note: The reliability of the prevention also depends on the Intrusion Prevention Level selected on Administration \rightarrow Local tab \rightarrow Operating Policies \rightarrow Intrusion Prevention \rightarrow Intrusion Prevention Level tab.

RF Propagation

The RF Propagation screen enables you to define default AP, Client, and Sensor antenna gain values.

			Jun 13 2011, 12:14:27 PM (GM1 +0530) [2] [2]	
🛱 Global 🎁 Local	🍈 Advanced - Default RF Propagation Set	tings		
	Default RF Propagation Settings			
Global Policies	Default Antenna Gain Values			
Event Settings	Define default SpectraGuard Sensor, AP and Client and the gain should be increased.	enna gain values. If better antennas are used,		
L Device Settings	Sensor Antenna Gain (dB)	2.3		
User Management	AP Antenna Gain (dB)	2.3		
Location Settings	Client Antenna Gain (dB)	0		
Auto Location Tagging	Transmitter Losses			
Location Tracking	Choose transmitter signal loss value in your environme power occurs due to antenna connectors, electromagne be different in different frequency bands. You can speci band.	int. When a device transmits, some loss in tic and environmental factors. This loss might ify the approximate transmitter loss in each		
	Loss at Source for 802,11a Transmitter (dB)	10		
Le System Settings	Loss at Source for 802.11b/g Transmitter (dB)	10		
WLAN Integration	-Signal Decay Values			
Construction	Choose signal decay values that define the attenuation of the signal in your environment. These values are dependent on the density of our environment.			
	For Nodes imported with SpectraGuard Planner			
	Minimum Signal Decay Constant	2		
	Maximum Signal Decay Constant	2		
	Signal Decay Slope (Beta)	0.08		
	Signal Decay Inflection (Alpha)	-4		
	Minimum Signal Decay Constant	2		
	Maximum Signal Decay Constant	2.5		
	Signal Decay Slope (Beta)	0.08		
	Signal Decay Inflection (Alpha)	-4		
	Signal Decay Slope (Beta) Signal Decay Inflection (Alpha)	0.08		

RF Propagation

Default RF Propagation Settings contains the following options:

- Default Antenna Gain Values: Specify the default sensor, AP, and Client antenna gain values. Antenna gain is a characteristic of an antenna used for transmitting or receiving signal, defined as gain in power when signal is received (or transmitted) using the antenna.
 - Sensor Antenna Gain (dB): Specifies the gain of antenna attached to the sensor. (Default: 2.3 dB)
 - AP Antenna Gain (dB): Specifies the gain of antenna attached to the AP. (Default: 2.3 dB)
 - Client Antenna Gain (dB): Specifies the gain of antenna attached to the Client. (Default: 0 dBm)

Note: If better antennas are used, you should increase the gain.

- Transmitter Losses: Select the transmitter signal loss value suited to your environment.
 - If your environment has metal or concrete walls, select a higher signal value.
 - If your environment has large spaces where the signal can propagate without much obstruction, select a lower signal loss value

When a device transmits, some loss in power occurs due to antenna connectors, electromagnetic, and environmental factors. This loss might be different in different frequency bands. You can also specify the approximate loss in each band.

- Loss at Source for 802.11a Transmitter (dB): (Default: 10 dB)
- Loss at Source for 802.11b/g Transmitter (dB): (Default: 10 dB)
- **Signal Decay Values:** Signal propagation depends heavily on environment. The obstacles present in environment might impede signal propagation, limiting its range. It is very difficult to accurately model signal propagation in all kinds of environment, but by fine-tuning the following four constants, you can more or less characterize your environment for signal propagation.

Note: The system uses the first set of parameters when the Planner file is imported; the second set for blank, gif, or jpeg files.

Minimum and **Maximum Signal Decay Constants** specify the range for the decay exponent, that is, the exponent at which signal decays with distance. **Signal Decay Slope (Beta)** and **Signal Decay Inflection (Alpha)** control how the decay exponent changes from its minimum value to maximum value.

- For Nodes with imported SpectraGuard Planner file:
 - Minimum Signal Decay Constant: (Default: 2.0 dBm)
 - Maximum Signal Decay Constant: (Default: 2.0 dBm)
 - Signal Decay Slope (Beta): (Default: 0.08 dBm)
 - Signal Decay Inflection (Alpha): (Default: -4 dBm)
- For Nodes with GIF, JPEG or Blank layout:
- Minimum Signal Decay Constant: (Default: 2.0 dBm)
 - Maximum Signal Decay Constant: (Default: 2.5 dBm)
 - Signal Decay Slope (Beta): (Default: 0.08 dBm)
 - Signal Decay Inflection (Alpha): (Default: -4 dBm)

Note: Planner models most significant objects; therefore Maximum Signal Decay Constant should be close to 2.0.

System Settings

Encoding

Select the language encoding (language setting) to be used to correctly display page encoded language text from the drop down list on the Encoding screen. Default is UTF-8. Parameters like SSID, when configured on the AP using page encoding (either non-english native window or using a language pack) will appear garbled when the page encoding does not match the encoding selected here.

Note: For the language encoding to be effective, it is mandatory to select **Multilingual** in the **Language Preference** field in **Administration** \rightarrow **Global** \rightarrow **GlobalPolicies** \rightarrow **User Management** \rightarrow **User Preferences** screen along with selection of language encoding from the drop-down list on the Encoding screen.

📰 Dashboard 💇 Events 😡 Devices 🏤 I	ocations 🖹 Reports 🔊 Forensics 🌉 Administration	Jun 13 2011, 12:18:27 PM (GMT +0530) 😰 😰 든 👰
💯 Global 🗊 Local	🐻 Encoding	
Dashboard 12 Events & Devices 11 Clobal Dicies Event Settings User Managenent Experts Auto Deletion Experts Server Manage Logs Manage Logs	ecations Reports Forensics Administration Fincoding Please select the language encoding to be used to correctly display page encoding Parameters like SSID, when configured on the AP using page encoding (either r will appear garbled when the page encoding does not match the encoding select Defaul (UTF-8) Apply Cancel	Jun 13 2011, 12:18:27 PM (GMT +0530) 2 2 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
 License Server Manage Logs View Logs Upgrade HA Status Login Configuration Wizards SpectraGuard Manager Configu WLAN Integration SpectraGuard SAFE 		

Encoding

Reports

The system can display a rich set of reports. The Reports screen enables you to modify the appearance and text in the generated reports. Refer to 'Adding a Report' in the Reports Tab section for more details.

Dashboard 💇 Events 🖕 Devices 🏠	ocations 🖹 Reports 🔊 Forensics 🌆 Administration	Jun 13 2011, 12:19:27 PM (GMT +0530) 🔯 💽 💽
🛱 Global 🗊 Local	Report Configuration	
111	Report Configuration	1
Global Policies	SpectraGuard Enterprise provides an easy to use facility to customize the look and feel of reports. Use this setting to modify the visual appearance and text in your reports.	
User Management	O Use default look and feel O Customize look and feel	
Location Settings	Report Header Report Summary Report Sections	
Le System Settings	Report Header	
Encoding	Left Aligned Header Text Tight Networks, Inc.	
Auto Deletion	Right Aligned Header Text Reports	
Vendors	Text Color Background	
SMTP	Report Title	
License	Title Text Report Name	
- 🕅 Server - 💜 Manage Logs	Text Color Background	
Image: Wiggrade Image: HA Status Image: Upgrade Image	Display Report Generation Information Display Report Description Text	
WLAN Integration WEAN Integration Rev ESM Integration Rev SpectraGuard SAFE		

Reports Configuration

Auto-deletion

The system is designed to store information about devices seen and older events over a period of time. The rate of growth of this information is dependent on the volatility of the wireless environment at the deployed location. This information also becomes obsolete after a certain time. It is necessary to delete this information periodically. Based on the event related configuration done by you, the system also raises and stores a number of events. If the configuration is such that there are significant number of events generated and stored, the stored event data size grows significantly faster. This event data also requires regular cleanup.

Auto Deletion allows you to specify values of various auto deletion parameters to control the frequency of deletion of information. The system generates an event for tracking the action of auto deletion. This event gives information only about device deletion. There is no event separately generated that indicates event deletion. Event deletion is also referred to as *Event Purging*.

💯 Global 🗊 Local	Auto Deletion Parameters		
() () () () () () () () () () () () () (et the parameters for automatic deletion of older	events and devices that	have been inactive for a long time.
🗭 Global Policies	Access Point Deletion Parameters		
🗄 📆 Event Settings	Select the category of APs and the number of da	ys of inactivity after which	APs should be automatically deleted.
🗄 🔃 Device Settings	Uncategorized	7 🗢 days [1 - 3	j.
🗄 🎲 User Management	Rogue	days [1 - 3	1
Location Settings	External	7 🖨 days [1 - 3	1
🙀 System Settings	Client Deletion Parameters		
Encoding	Select the category of Clients and the number of	days of inactivity after w	nich Clients should be automatically deleted.
Reports	Uncategorized	7 🗘 days [1 - 3	1
Auto Deletion	Authorized	days [1 - 3	1
Vendors	External	30 🜲 days [1 - 3	1]
😼 SMTP	Rogue	days [1 - 3	1
License	☑ Guest	7 🗘 days [1 - 3	0
Server	Network Deletion Parameters		
👹 Manage Logs	Specify how long exposed networks should be re	tained in the database.	
📲 🔞 View Logs	No. of days to retain exposed Networks	30 🗢 days[1 - 90]	
💕 Upgrade	Events Deletion Parameters		
HA Status	Specify the maximum number of events that woo Note: Events in excess of these are deleted from not expired.	Ild be retained on the ser the server even if the tin	ver. le period for retention mentioned below has
Wizards	Max. Security Events	50,000 🗢 [0 - 80000	1
SpectraGuard Manager Configu	Max. Performance Events	10,000 🗘 [0 - 40000	1
WLAN Integration	Max. System Events	1,000 🗘 [0 - 2000]	
ESM Integration	Specify how long events should be retained in th Note: Events older than the period specified will I than the numbers mentioned above.	e database. se deleted from the datab	ase even if the number of events are smaller
	Max. days for which to retain Events	30 🗢 days [1 - 3	5]
	Apply Cancel Restore Defaults		

Auto Deletion

The Auto Deletion Parameters window contains the following options:

• Access Point Deletion Parameters: Select the checkboxes to choose the category of APs that you would like the system to delete automatically. Specify the number of days of inactivity after which the AP records are automatically deleted.

(Minimum: 1 day; Maximum: 30 days)

- Uncategorized
- > Rogue
- External

Note: Authorized APs are not auto deleted from the system. If you want to delete inactive authorized Access Points, you have to delete them manually.

• Client Deletion Parameters: Select the check boxes to choose the category of wireless Client devices that you would like the system to automatically delete. Specify the number of days of inactivity after which the wireless Client records are deleted automatically.

(Minimum: 1 day; Maximum: 30 days)

- Uncategorized
- > Authorized
- External
- Rogue
- Guest

• **Network Deletion Parameters:** Select the **No. of days to retain exposed Networks** check box and specify the duration, in days, for which the exposed networks are to be retained on the server.

(Minimum: 1 day; Maximum: 90 days; Default:30 days)

• Events Deletion Parameters: Specify the maximum number of events that would be retained on the server.

Maximum Security Events

(Minimum: 20000; Maximum: 80000; Default: 50000)

Note: Maximum number of security events that can be retained for SA-350 appliance, is 0.7 million.

> Maximum Performance Events

(Minimum: 5000; Maximum: 40000; Default: 10000)

Note: Maximum number of performance events that can be retained for SA-350 appliance, is 0.25 million.

Maximum System Events (Minimum: 500; Maximum: 2000; Default: 1000)

Note: Maximum number of system events that can be retained for SA-350 appliance, is 0.05 million.

Specify how long events should be retained in the database.

Maximum days for which to retain Events (Minimum: 1 day; Maximum: 365 days; Default: 30 days)

(wininitum: 1 day, waxintum: 505 days, Default: 50 days)

Note: Events older than the period specified will be deleted from the database even if the number of events are smaller than the numbers mentioned above.

Auto Deletion Action

You can track auto deletion of inactive APs, Clients, and events, by monitoring the special event generated by the system. The system generates an event containing the summary of the actions performed during the Auto Deletion operation, if and only if any physical deletion of information actually took place.

Vendors

The **Vendors** screen enables you to view a list of vendors with their MAC prefixes. The 3-byte MAC prefix typically identifies the vendor for any given 802.11 device.

				_	
🕼 Global 🕼 Local	Vendor Configuration				
	802.11 Vendor Configuration				
Global Policies	The 3 byte MAC prefix typically ide	ntifies the vendor for any given 802.	1 device.		
Fyent Settings	A list of popular vendors is shown l	below. You can add custom vendor na	ames to		
1 Danier Coming	the list.				
PL Device seconds	Vendor Name	MAC Prefix		Add	
User Management	11wave	00:0B:10	-	Delater	
Continue Settings	Inet-Corp	00:30:70	3	Invicience. 1	
Le System Settings	2001-Tech	00:11:B2			
Encoding	2wcom	00:11:99			
Ph Circoding	2Wire	00:0D:72			
Reports	2Wire	00:D0:9E			
Auto Deletion	2Wire	00:14:95			
Vendors	2Wire	00:12:88			
SMTP	2Wire	00:18:3F			
mil	2Wire	00:19:E4			
License	2Wire	00:1A:C4			
- 🗟 🖌 Server	2Wire	00:1B:5B			
- Manage Logs	2Wire	00:1E:C7			
Wew Logs	2Wire	00:1F:B3			
st	2Wire	00:21:7C			
er upgrade	2Wire	00:22:A4			
HA Status	2Wire	00:23:51			
	2Wire	00:1D:5A			
Wizards	2Wire	00:24:56			
	2Wire	00:25:3C			
SpectraGuard Manager Configu	2Wire	00:26:50			
WLAN Integration	2Wire	34:EF:44			
ESM Integration	2Wire	B0:E7:54			
The Spectra Guard SAFE	2Wire	3C:EA:4F			
	2Wire	98:2C:BE			
	2Wire	C0:83:0A			
	3Com	00:04:0B			
	3Com	00:D0:D8			
	3Com	00:06:8C			
	3Com	00:02:9C			
	3Com	00:0A:04			
	3Com	00:0E:6A			
	3Com	00:26:54	100		

Vendors

To add a new pair of vendor name and MAC prefix, click **Add**. The Add Vendor dialog opens. Specify the Vendor Name and the MAC Prefix and click **Add**.

Add Vendor					×
Vendor Name	1				
MAC Prefix					
-		10		-	 _
_	Add		Can	cel	

Add Vendor Dialog

To delete any pair from the existing list, select the relevant row and click **Delete**.

SMTP

The SMTP screen enables you to set Simple Mail Transfer Protocol (SMTP) server settings to send emails when events occur. You must have administrator privileges to set these values.

Dashboard 👷 Events 🕼 Devices	Locations B Reports C Forensics Adr	ministration	Jun 13 2011, 12:27:27 PM (GMT +0530) 🔯 🕐 든 🧕
🛱 Global 🕅 Local	🔒 SMTP Configuration		
	SMTP Configuration		
Diobal Policies Die Event Settings	Enter the SMTP settings below. These se and password recovery. Leave the SMTP The value "Email Address in From Field" that are sent by the Server.	ttings will be used to send email for events, reports ' settings blank if you do not wish to receive email, is shown in the From address of the email messages	
User Management	SMTP Server IP Address/Hostname	127.0.0.1	
Location Settings	Port	25	
Bystem Settings	Email Address in From Field	server@localhost.localdomain	
Encoding	Authentication Required		
Reports	User Name		
Auto Deletion	Password		
Vendors		Test SMTP Settings	
- Ca SMTP	Server Access URL		
License	Enter URL to access this Server.		
👫 Server	Server Access URL http://www.http	ps://wifi-security-server	
Upgrade HA Status HA Status Login Configuration Wizards Wizards Wizards Wizards Wizards Wizards Wizards SpectraGuard Manager Configuration Mag SpectraGuard SAFE			

SMTP

Note: If you want the system to notify you by an events email, you need to specify SMTP server details. The system does not email events by default. If you do not want to receive email for the events, select **Restore Defaults** and **Apply**.

SMTP Configuration contains the following options:

• **SMTP Server IP Address/Hostname:** Specifies the IP Address or the Hostname of the SMTP server used by the system for sending email alerts.

(Default: 127.0.0.1:25)

The following are the authentication protocols for SMTP server:

- PLAIN (For sendmail 8.10 and above)
- LOGIN (For sendmail 8.10 and above)
- > NTLM (Windows proprietary authentication method)
- **Port:** Specifies the Port number of the SMTP server used by the system for sending email alerts.
- Email Address in From field: Specifies the source address from which email alerts are sent.
- Authentication Required: If enabled, specifies whether the SMTP server requires authentication.
 - **Username**: Specifies the user name for SMTP server authentication.
 - > **Password**: Specifies the password for SMTP server authentication.

To send a test e-mail, click **Test SMTP Settings**. The settings used for this mail are those that you have specified.

License

You can upgrade your current version to enable or disable features by a new license key. The **License Update** screen enables you to change the license key. To update the license, click Browse and navigate to the location of the License Key File. To finish, click Apply.

Note: To apply the license effectively, logout and re-login to the console.



License

Server

The Server screen enables you to view server information.

📰 Dashboard 💇 Events 🧔 Devices 🏤 L	ocations 🖹 Reports 🔊 Forensics 🌆 Adm	inistration	Jun 13 2011, 12:31:29 PM (GMT +0530) 🕐 🕐 🚍 💽
🗊 Global 🗊 Local	🚯 Advanced - Server		
	Server Details		
🗊 Global Policies	Server ID	1	
Event Settings	Port	3851	
Device Settings	Max Sensors Allowed (Physical Devices)	100	
User Management	Allowable Conversions to AP	50 of 100	
Location Settings	IPv6 status	Enabled	
E 🙀 System Settings	Server Status		
Encoding			
Reports	Current Status	Running	
Auto Deletion		Stop Sporter-Guard Enterprise Service	
Vendors	Change Status	Sup speciaddard chicephise server	
SMTP			
License			
Manage Logs			
🗰 🕼 View Logs			
Upgrade			
HA Status			
Wizards			
SpectraGuard Manager Configu			
WLAN Integration			
ESM Integration			
🗄 🚺 SpectraGuard SAFE			
< >			

Server Details

• Server Details: This is a read-only section and displays the following information:

Server ID: Unique identifier for the server appliance. If you have installed a single server appliance, then retain the default server ID, that is, **1**.

- > **Port**: The User Datagram Protocol (UDP) port number used.
- Max Sensors: Maximum number of sensors that can connect to the server.
- **Max Sensor/AP Combos**: Maximum number of sensors that can be converted to Sensor/AP Combo devices. This is derived from the license. If you do not have a license for Sensor/AP combo device, this field will not be seen.
- > **IPv6 status**: Indicates if IPv6 is enabled on the server.

• Server Status: Enables you to view the Current Status of the server – Running or Stopped. The administrator can Change Status, that is, start or stop the server.

• **RAID Status:** Enables you to view the **Current Status** of the RAID Array – **Normal, Rebuilding, Degraded,** or **Failed.**

Manage Logs

The system keeps log of user activities. Under **Manage Logs**, you can specify in the **User Action Logs Deletion Threshold** field, the number of days for which logs history is to be maintained, before deleting it automatically. (*Minimum: 7 days; Maximum: 365 days; Default: 30 days*)

Dampoard O cours @ courses @ co	cations 📴 Reports 🔊 Forensics 🦉 Administration	Jun 13 2011, 01:45:45 PM (GMT +0530) 😰 💽 🛃 🛃
💯 Global 🗊 Local	👔 Manage Logs	
Clobal Pelicies Coobal Pelicies Coobal Pelicies Coobal Pelicies Coobal Pelicies Coobal Pelicies Coobal Pelicies Coobal Pelicies Coobal Pelicies Coobal Pelicies Coobal Pelicie	Cations Reports Connexics Administration Wanage Logs SpectraGuard Enterprise keeps log of system activities. Specify the number of days for which logs history be maintained, before deleting it automatically. User Action Logs Deletion Threshold 00 © days [7 - 365] User Action Logs Deletion Threshold 00 © days [7 - 365] Performed activities	Jun 13 2011, 01:45:45 PM (GMT +0530) î 🕃 🖗 🖿

Manage Logs

View logs

The system enables downloading the user action logs for review. Only the superuser has permission to download logs. Logs can be downloaded as .TSV (tab separated values) or .CSV (comma separated values) format. The .TSV format is also called Unicode format. The downloaded file can be viewed using text editors such as Excel, WordPad etc.

Under **Time Filter**, click the calendar icon **m** to specify the **Time Period**. Only those records in the logs which fall in the selected time period will then be included in the downloaded log file.

Under **Filter By**, it is possible to select a type of log records which are to be downloaded. When such specific type is selected, log records of only that type will be included in the downloaded log file. By default, records of all types are included.

Under **Sort By**, it is possible to select a specific column on which the records in the downloaded file are to be sorted. By default, the sorting is done on date and time.