Monitor Extreme Access Control Health in Extreme Management Center

The following sections provide detailed information on how to use specific Extreme Management Center reports and NAC Manager features to monitor Extreme Access Control health. These reports provide you with the information you need to monitor, analyze, and troubleshoot Extreme Access Control problems.

- Monitor Extreme Access Control Engine Performance
- Monitor Extreme Access Control Engine Memory Use
- View Extreme Access Control Engine Historical Data
- Monitor Extreme Access Control Critical Events
- Monitor Extreme Access Control Engine Load
- Monitor Extreme Access Control End-System Health
- Create Alerts with Extreme Access Control Notifications
- Verify Extreme Access Control RADIUS Configuration
- Extreme Management Center Custom Reports

Monitor Extreme Access Control Engine Performance

The Extreme Access Control engine Device Availability report provides a historical overview of the engine status. The report shows at-a-glance when an engine is offline, or whether an engine is consistently on and offline over time. The report lets you quickly determine the specific date when an engine is unavailable without having to review log data to determine the date.

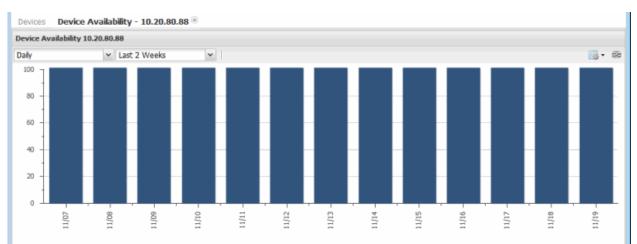
For a backup engine, the report can provide a good indication of possible engine or network issues that may go otherwise undetected until the moment when the engine is needed. If the report indicates a problem, review the Extreme Access Control engine logs for the dates in question (see <u>Extreme Access Control Engine Log Locations</u>), to gain additional insight into the possible root cause of the problem.

Access the Device Availability report from the **Network** tab. Right-click on an Extreme Access Control engine and select View Device Details > System > Device Availability, as shown here.

•						
Status	IP Address	Display Name	D	evice Type	Family	Firm
•	10.20.88.100	10.20.88.100	N	etSight Suite Appliance	NetSight Applian	4.4.
•	10.20.80.38	10 20 80 38	F	terasys NAC Gateway	Security Applian	4.3.
•	10.20.82.2	View Interfaces		2524	HP	F.02
•	10.20.80.3	Security Assessment		terasys NAC Appliance 2K	Security Applian	4.3.
•	10.20.80.9	Choose FlexView		G124-24	C-Series	06.0
•	10.20.80.8	Launch WebView		terasys NAC Gateway	Security Applian	4.4.
•	10.20.80.7			582-51	Matrix E-Series	03.0
•	10.20.80.6	Collect Device Statist	DCS	itrix N1 Platinum	Matrix N-Series	06.1
•	10.20.80.2	Refresh Devices		terasys NAC Gateway I	Security Applian	4.4.
•	10.20.80.88	Firmware	Þ	terasys NAC Gateway	Security Applian	4.4.
•	10.20.86.30	Enterasys Support	Þ	G124-24	C-Series	06.0
•	10.20.80.8	View Device Details	Þ	Alarms 🕨		7.7.
•	10.20.80.80	Add To Man		System 🕨	Davies Availab	
•	10.20.80.1	Add To Map	_	oyoum	Device Availab	
•	10.20.86.25	10.20.86.25	с		Host Processor	Load
•	10.20.80.14	10.20.80.14	с	VLAN Þ	Host Resource	s
•	10.20.80.13	10.20.80.13	с	NAC 🕨	Host Storage	

Accessing the Device Availability Report

The Extreme Access Control engine Device Availability report is displayed in a new tab, as shown below.



Device Availability Report

Monitor Extreme Access Control Engine Memory Use

The Extreme Management Center Host Resources report lets you monitor physical, virtual, and swap memory usage on an Extreme Access Control engine.

As you monitor an engine's physical and virtual memory, keep in mind that it is common for Linux-based systems (such as the Extreme Access Control engine) to show high memory utilization. Once a process consumes memory, the memory remains allocated to the process under the assumption it may be required in the future. If a different process calls for that memory, and it is not in use, it is made available.

It is also important to monitor swap memory statistics for your Extreme Access Control engines. When an engine starts using swap memory, it indicates a potential issue, and more active monitoring of the engine may be required. Running commands such as the "top" command (see <u>Linux "top" Command</u> section under NAC Troubleshooting) provides more accurate and up-to-date information on whether swap memory is actively being used, and which processes are consuming the highest memory and CPU.

Use the **Network** tab to access the Host Resources report for an Extreme Access Control engine. Right-click on an Extreme Access Control engine and select View Device Details > System > Host Resources, as shown here.

vices									
-									
Status	IP Address	Dis	play Name	Device	Туре		Famil	y	Firmware
•	10.20.80.6	10.	20.80.6	Matrix I	V1 Pla	tinum	Matri	x N-Series	06.11.01.0
•	10.20.80.88	**			(s NA	C Gateway	Secur	ity Applian	4.4.0.57B
•	10.20.86.30	1	View Interface	S	-24		C-Ser	ies	06.03.04.0
•	10.20.80.83		Security Assess	sment					7.7.3
•	10.20.80.80		Choose FlexVie	sw	SR		Smart	tSwitch 2000	05.08.04
•	10.20.80.16		Launch WebVie	ew.	/s NA	C Controller	Secur	ity Applian	06.11.01.0
•	10.20.86.25		Collect Device	Statistics	-24		C-Ser	ies	06.03.04.0
•	10.20.80.14		Refresh Device		-48		C-Ser	ries	05.02.08.0
•	10.20.80.13		Kerreshipevice		-48		C-Ser	ies	05.02.08.0
•	10.20.80.78		Firmware	Þ	/s NA	C Gateway I	Secur	ity Applian	4.3.0.DEV
•	10.20.80.12		Enterasys Supp	port 🕨	-24		C-Ser	ies	06.03.04.0
•	10.20.80.10		View Device De	tails 🕨		Alarms	, brit	x N-Series	07.62.02.0
•	10.20.88.169		Add To Map			System	P.	Device Av	alahitu
•	10.20.85.11	-	Add To Map	LITTLE DE	_	Interface	Þ		
	10.20.85.10	10.	20.85.10	Enteras		VLAN	1		essor Load
•	10.20.80.129	10.	20.80.129	C3G124		VLAN		Host Reso	ources dhy i

Accessing the Host Resources Report

A Host Resources report for the Extreme Access Control engine is displayed in a new tab, as shown below.

Host Resources Report



View Extreme Access Control Engine Historical Data

The NAC History report provides a detailed view of the overall Extreme Access Control engine load based on critical Extreme Access Control functions including authentication requests, captive portal statistics, and connected agents. The report displays the latest load data as well as minimum, maximum, and average statistics for an overview of activity by function. This provides a historical view for each individual engine and is similar to the <u>Extreme Access</u> <u>Control Engine Load report</u>, which presents current load data for all engines.

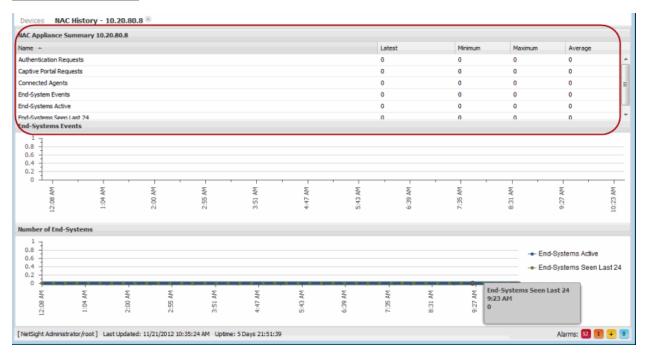
In Extreme Management Center, select the **Network** tab. Right-click on an Extreme Access Control engine and select View Device Details > NAC > NAC History, as shown here.

Accessing the NAC History Report

									Show Filters Search	1		×
Status	IP Address	Display Name	Device		Family	Firmware	Updates	Boot PROM	Base MAC	Chassis ID	Stats	Location
				-,							•	
	10.20.80.9	10.20.80.9	C3G12	4-24	C-Series	06.03.04.0004		01.00.49	00:11:88:A9:19:A0	07410756225F	4	NetSigh
٠	10.20.80.8			sys NAC Gateway	Security Applian	4.4.0.35T		N/A	00:04:23:85:61:5A		1	unknow
•	10.20.80.7	View Interfaces		51	Matrix E-Series	03.07.33		01.02.00	00:01:F4:89:09:60	02080349210F	1	NetSigh
•	10.20.80.6	Security Assess	nent	V1 Platinum	Matrix N-Series	05.11.01.0040		01.00.15	00:11:88:31:F6:EB	STATEN_ISLAN	~	NetSigh
•	10.20.80.28	Choose FlexView	v	ys NAC Gateway I	Security Applian	4.4.0.DEV		N/A	00:21:9B:89:A4:1C		1	Unknow
•	10.20.80.88	Launch WebView	v	ys NAC Gateway	Security Applian	4.4.0.578		N/A	00:11:88:FB:CB:D2		~	unknov
•	10.20.86.30	Collect Device S	tatistics	4-24	C-Series	06.03.04.0004		01.00.49	00:11:88:8F:88:DF	07410754225F	~	
•	10.20.80.83	Refresh Devices		e		7.7.3		5)	00:04:96:00:39:60	0317500542	~	Unknow
•	10.20.80.80	Kenebridende		25R	SmartSwitch 2000	05.08.04		02.01.06	00:E0:63:4C:45:F4	Stand Alone	1	
•	10.20.80.16	Firmware	Þ	sys NAC Controller	Security Applian	06.11.01.0033		01.00.21	00:11:88:FA:9C:09	08476380635B	1	
•	10.20.86.25	Enterasys Supp	xt ⊧	4-24	C-Series	06.03.04.0004		01.00.49	00:11:88:B4:BE:1F	08161462225F	~	NetSigh
•	10.20.80.14	View Device Det	ais 🕨	Alarms	Series	05.02.08.0006		01.00.47	00:11:88:1B:6B:D9	05341457900E	~	NetSig
•	10.20.80.13	Add To Map		System	Series	05.02.08.0006		01.00.47	00:11:88:65:1E:7A	06460682905J	~	NetSigh
•	10.20.80.78	20120100170		Interface	scurity Applian	4.3.0.DEV		N/A	00:1E:C9:BB:F3:A7		~	unknov
•	10.20.80.12	10.20.80.12	C3G12		Series	06.03.04.0004		01.00.49	00:11:88:B4:BE:00	08161462225F	~	NetSig
•	10.20.80.10	10.20.80.10	Matrix	NAC	1			01.00.19	00:11:88:E3:23:5D	08075361635E	~	NetSigh
•	10.20.88.169	10.20.88.169	G3G12		NAC Histor)	01.00.46	00:00:12:10:09:08	11141222	1	Locatio
4 Pa	ge 1 of 3		Reset	Bookmark	NAC End-S	System Access States				Displavir	ng Devices	1 - 50 of

The NAC History report is displayed in a new tab, as shown below. Look at the NAC Appliance Summary report for engine load data.

NAC History Report



Monitor Extreme Access Control Critical Events

The Extreme Access Control report on Most Severe Extreme Access Control Events displays the 10 most severe Extreme Access Control events. If the most recent events indicate a current issue, further in-depth review of the events may be required. A good place to start would be the server.log on the Extreme Management Center server (see Accessing the Server Log File in the Extreme Management Center Troubleshooting section of the Extreme Management Center Troubleshooting section of the Extreme Access Control engine (see Extreme Access Control engine Log Locations). Depending on the error, additional debug options may be required to obtain more in-depth log data. For more information, see Extreme Access Control Troubleshooting.

In Extreme Management Center, select the **Reports** tab. Expand the Identity and Access - Health folder and select the report.

Console	Timestamp	Severity	Information
Custom	5/20/2013 3:18:16 PM	•	Appliance 10.20.88.27 running version 4.4.0.105 does not support Collect NAC Status capability.
custom	5/20/2013 3:18:16 PM	•	Appliance 10.20.80.29 running version 4.3.0.108 does not support Collect NAC Status capability.
Data Center Manager	5/20/2013 3:18:16 PM	•	Appliance 10.20.88.128 running version 4.4.0.115 does not support Collect NAC Status capability.
Device	5/13/2013 10:42:02 PM	•	Audit found errors for NAC Appliance: 10.20.88.27, NAC Appliance is Unreachable
Flows	5/13/2013 10:42:02 PM	•	Audit found errors for NAC Appliance: 10.20.88.128, NAC Appliance is not assigned to this management server: 10.20.88.1
	5/13/2013 10:42:02 PM	•	Audit found errors for NAC Appliance: 10.20.80.29, NAC Appliance is not assigned to this management server: 10.20.88.15
Identity and Access - Dashboard	5/7/2013 1:50:36 AM	•	Audit found errors for NAC Appliance: 10.20.88.27, NAC Appliance is Unreachable
Identity and Access - Health	5/7/2013 1:50:36 AM	•	Audit found errors for NAC Appliance: 10.20.88.128, NAC Appliance is not assigned to this management server: 10.20.88.1
Access States	5/7/2013 1:50:36 AM	•	Audit found errors for NAC Appliance: 10.20.80.29, NAC Appliance is not assigned to this management server: 10.20.88.15
End-Systems by Vulnerability	5/7/2013 1:49:03 AM	۰	Audit found errors for NAC Appliance: 10.20.88.27, NAC Appliance is Unreachable
💼 High Risk by Week			
Highest Risk End-Systems			
Most Frequent Vulnerabilities			
Most Severe NAC Events			

Most Severe NAC Events Report

Monitor Extreme Access Control Appliance Load

The Extreme Access Control Appliance Load report provides a summary of endsystem usage for each Extreme Access Control engine on the network, including the number of active end-systems on the engine, and the number of authentication and captive portal requests per minute.

This report is useful for determining whether action may be required in order to more evenly distribute the client load among available Extreme Access Control engines. The report shows which engine may have too many end-systems authenticating against it and which engine may be underutilized and available to handle additional end-system requests. The report also provides helpful information for capacity planning and determining future needs for additional Extreme Access Control hardware.

In Extreme Management Center, select the **Control** tab. Click on **System** to view the Appliance Load report.

									6
Overview			Top Switches by B	End-Systems		System Events			
Total End-Systen	5:	1002	Switch IP	End-Systems		Timestamp	Severity	Information	
Active Last 30 Da	y5:	1	10.20.88.8	1		07/31/12 9:33:57 AM		Failed to enforc	1
Health Results/Vu	nerabilities:	4087/19612				07/31/12 9:33:47 AM	•	Failed to enforc	
MAC Registered L	sers:	11				11/20/12 1:00:00 AM	•	Agent-based as	
NAP Capable:		0.0%				11/20/12 1:00:00 AM	0	Agent-based as	
NAP Capable.		0 0.0%				11/20/12 1:00:00 AM	•	Agent-based as	
						11/20/12 1+00+00 AM	~	Acapthaced ac	_
Name		stems Active	Seen Last 24 Hours	End-System Ev		thentication Requests/min		e Portal Requests/mir	n
Name	End-Sy	stems Active	Seen Last 24 Hours	End-System Ev	vents/min Au	thentication Requests/min	Captiv	e Portal Requests/mir	n
10.20.80.37	2		2	0.4	0.	2	0		_
10.20.85.10	0		0	0	0		0		
10.20.88.101	0		0	0.37	0		0		
10.20.80.39	0		0	0	0		0		_
Appliance Inform	ation		Top Appliances B	y End-Systems		Total End-Systems			
	ne	Appliance Group				1200 7			
IP Address Na		Randy *	NACDEMO - naca2k_8022 -			800			
	a2k_8022					600 - 400 -			
10.20.80.22 na	a2k_8022 20.80.28	Default 🗏	172.16.1.38 -			400 -			
10.20.80.22 na 10.20.80.28 10	-	Default	172.16.1.38 -			200 -			
10.20.80.22 na 10.20.80.28 10 10.20.80.32 10	20.80.28	C'ETBOIL				200	11/16	11/17 11/18 1	1/1

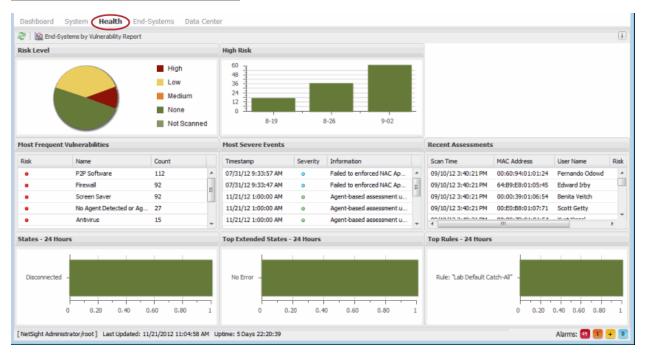
Appliance Load Report

Monitor Extreme Access Control End-System Health

The Extreme Access Control Health reports provide information on overall endsystem health.

The Risk Level report helps you quickly determine the overall status of threats and vulnerabilities to the entire Extreme Access Control environment. Select a specific section of the chart to launch a report of all end-systems that meet that criteria. Select the "High" portion of the chart to display a report of all endsystems that have a high-risk vulnerability. The Most Frequent Vulnerabilities report lists the top vulnerabilities detected and the number of end-systems reporting that vulnerability. This report is useful in identifying specific areas of the user environment that may need immediate attention, or in determining the scale of a specific vulnerability.

In Extreme Management Center, select the **Control** tab. Click on **Health** to view the end-system reports.



Identity and Access Health Reports

Create Alerts with Extreme Access Control Notifications

Extreme Access Control Notifications let you create alerts for when specific events or triggers take place in Extreme Access Control. Each notification can be defined for a specific type and trigger. The notification type defines the source of the event that activates the notification, such as end-system, end-system group, user group, or health result. The trigger determines when a notification action is performed, based on filtering for a specific event. For example, if you select end-system group as your type, the trigger may be when entries in the group are added or removed.

Notifications can be further defined by specific conditions that, in addition to the trigger, determine when actions are performed. For example, you can

configure a condition that filters notifications based on selected engines, user groups, and device groups, as well as Extreme Access Control profile, time, and location.

Notifications can have a variety of actions configured such as sending an email, generating a syslog message, sending an SNMP trap, or launching a custom program or script. Email notifications can be customized so that only certain groups are notified for specific events based on the selected mailing list.

In NAC Manager, click on the Notifications toolbar icon and use the Manage Notifications window to create your notifications.

Elle Tools Applications	Help	-				
🖳 🗱 🗖 🏭 🎤 🍳	(🕲 🏚		12			
Appliance Groups Appliance Groups Appliance Groups Statistics						
Manage Notifications Manage your NAC notifications including enabling, adding, editing, and testing specific notification rules. Notifications enable alerts as well as integrate with existing IT workflows.						
	Manage you	r NAC notifications in enable alerts as we			cific notification rules.	
	Manage you	r NAC notifications in enable alerts as we			cific notification rules.	
	Manage you Notifications	r NAC notifications in enable alerts as we Name	I as integrate with	existing IT workflows.	4	
	Manage you Notifications	r NAC notifications in enable alerts as we Name Name NetSight event Re	I as integrate with	existing IT workflows.	Action Send Email to Helpdesk a	
	Manage your Notifications	NAC notifications in enable alerts as we Name NetSight event Re Report Blackliste	I as integrate with Type End-System	existing IT workflows. Trigger Quarantine End-System	Action	

Manage Notifications Window

Here are some examples of how notifications can be used to alert you of changes or events in NAC:

- Send an email to the Help desk when an end-system changes location, for example if it moves from a wired connection in a building to a wireless connection outside.
- Send a trap if an end-system fails registration.
- Send a syslog message if an end-system reports a high-risk assessment result.
- Send an email if an end-system that is reported as a stolen laptop authenticates on the network.
- Send an email if someone logs into the network after normal work hours.
- Send an email when an end-system is added or removed from an end-system group, such as the Blacklist end-system group or another defined end-system group.
- Send an email when a user is added or removed from a user group, such as an Administrator or Help Desk user group.

For more information, see the Manage Notifications window and Edit Notification Action window Help topics in the NAC Manager User Guide.

Verify Extreme Access Control RADIUS Configuration

Use the NAC Manager Verify RADIUS Configuration tool to ensure that the RADIUS configurations on your switches are consistent with your Extreme Access Control configuration. The verify operation alerts you to any RADIUS configurations that are out of sync and could cause RADIUS authentication problems on the network.

Switch RADIUS configurations can be modified independently of Extreme Access Control; for example, they can be manually edited through the CLI, through Policy Manager, or by applying an archived switch configuration that was archived prior to the device being added to NAC Manager. This can cause an authentication failure or a loss of visibility to the devices on the network. The Verify RADIUS Configuration tool can help you troubleshoot this problem.

For more information, see How to Verify RADIUS Configuration in the NAC Manager User Guide.

In NAC Manager, right-click on an engine and select Verify RADIUS Configuration as shown here.

Accessing Verify RADIUS Configuration

ie Icols Applications Help	* 🗾 🕫	🤞 💷 🙆 🏠	lati (mi mi	[(h.)
Al NAC Appliance Groups Al NAC Appliances	Vvek	come End-Systems		1
		Name	IP Address	Appliance Type
	10	Find		teway
	10	Filter		teway
	10 10 17	Sort		teway teway
	10	Auto Export		teway
	17	Delete Appliance		teway
	na		A	teway
	10	Change Appliance		teway
	NA.	Manage Appliance	Certificates	teway
	10	Verify RADIUS Con	rtiguration	teway
	10	Collect NAC Status		teway
	10	Launch CPU Utilizat	tion View	teway
	10		Diskspace Utilization \	teway
	10		Diskspace Otilization Y	teway
		Select All		
		Table Tools		•

Verification results are displayed in the Verify RADIUS Configuration window.

Verify RADIUS Configuration Window

Switch IP Address	Status	Result	Details
0.20.80.10	Verify Complete	Failure	Primary RADIUS should be "10.20.80.34" instead of "10.20.80.37".
0.20.88.8	Verify Complete	Failure	RADIUS Authentication should be enabled. Primary RADIUS should be "10.2
0.20.88.8	Pending		
0.20.82.3	Verify Complete	Failure	Switch does not support RADIUS MIBs.
<			,
Done			Show O Differences Only O Al

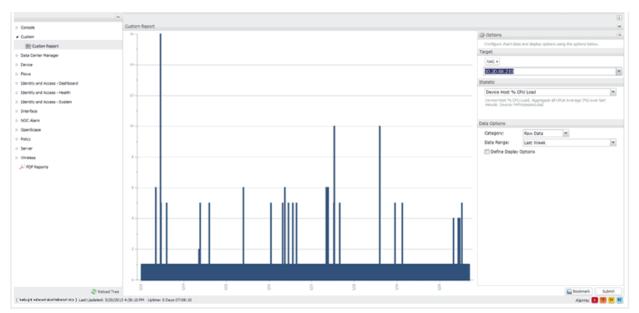
Extreme Management Center Custom Reports

Extreme Management Center Custom Reports let you create specialized reports for monitoring Extreme Access Control engine performance. Create reports on a variety of Extreme Access Control engine statistics including CPU load, disk usage, memory usage, and device availability. Individual reports of interest can be bookmarked for ease of use in accessing the desired information.

On the **Reports** tab, expand the Custom folder and select Custom Report. Use the Options panel to configure your custom report by selecting a report target (such as Extreme Access Control), the statistic to monitor (such as CPU utilization), and the time period and date range to display. Click the **Submit** button to generate the report. An example report on Extreme Access Control engine CPU utilization is shown below.

TIP: CPU usage can be monitored more closely in real-time using diagnostic tools such as the Linux "top" command.

Extreme Management Center Custom Report



3/2018 8.1 Revision -00 PN: 9035442 Contents Subject to Change Without Notice

Configure RADIUS Clients to Monitor Extreme Access Control Engines in Extreme Management Center (Legacy)

This Help topic tells you how to configure RADIUS monitoring tools to monitor Extreme Access Control engine performance and availability.

Use the following steps to create a list of RADIUS monitoring clients and configure a special authentication mapping for your AAA configuration used to authenticate the clients.

If you have multiple engine groups, you can use the same tools to monitor different engine groups, but each engine group is configured separately.

- 1. Select the All Appliances group or an individual engine group in the NAC Manager left-panel tree.
- 2. In the right-panel **Configuration** tab, click on the **Edit** button in the RADIUS Monitor Clients field.

Configuration Switches	End-Systems NAC Appliances Statistics
Appliance Group - Def	ault
Appliance Settings:	Default
Appliance Count: 2	2
Load Balancing:	Disabled Edit
RADIUS Monitor Clients:	
	Defsuit Edit
Default Profile:	Default NAC Profile
Registration:	Enabled
Assessment/Remedia	tion: Disabled
Portal Configuration:	Default
AAA Configuration:	Default

3. The Configure RADIUS Monitor Clients window opens.

Configure DADRIC Maniher Climate Default
Configure RADIUS Monitor Clients - Default
RADIUS monitoring tools used to monitor all the NAC appliances in this appliance group.
RADIUS Monitor Clients
192.0.2.14
198.51.100.23
Shared Secret
Server Shared Secret:
Verify Shared Secret: ************
Show Shared Secret
OK Cancel Help

- 4. Use this window to create a list of the monitoring tools (clients) used, and specify the shared secret to be used for all of them.
 - a. Click the 💷 button. Enter the IP address for the first client and click **OK**. Repeat for each client that you want to add.
 - b. Enter the Server Shared Secret used. This is a string of characters used to encrypt and decrypt communications between the RADIUS Monitor clients and the engines. This string must match the shared secret configured on the client. Without the shared secret, the engines and clients will be unable to communicate. The shared secret must be at least 6 characters long; 16 characters is recommended. Dashes are allowed in the string, but spaces are not.
 - c. Re-enter the shared secret to verify it.
 - d. Click OK.
- 5. Use the NAC Manager 🍩 toolbar button to open the NAC Configuration window or use the **Edit** button in the **Configuration** tab.

6. Select the AAA configuration in the left panel.

NAC Configuration: Defa	
Edit NAC Configurations to m	AAA Configuration: Default = AAA Configuration: Default = Authenticate Requests Locally for MAC (PAP), MAC (MsCHAP) = Local Password Repository: Default =
	Authentication Type User/MAC/Host Match Location Authentication Methy Any Any Proxy RADIUS
	•
	Save Close Help

- 7. In the right-panel mapping table, click the button to add a new mapping. (You must be using an advanced AAA Configuration in order to see the mapping table. If you are not, right-click on the AAA Configuration and select **Make Advanced**.)
- 8. The Add User to Authentication Mapping window opens.

Add User To Authentication Mapp	ing 💌
Authentication Type:	RADIUS Monitor
User/MAC/Host: Pattern Group 	*
Location:	Any T
Authentication Method: Local Au	thentication +
Password For All Authentication	
Password:	
LDAP Configuration: None	×
LDAP Policy Mapping: Default	*
	OK Cancel Help

- a. Set the Authentication Type to RADIUS Monitor.
- b. Set the Authentication Method to Local Authentication and select the Password for all Authentications checkbox. Enter the desired password that will be used for all client authentications.
- c. Click OK.
- 9. The new mapping will be listed in the mapping table. You can use the arrows to adjust the position of the new mapping in the table. In the screen below you can see that the RADIUS Monitor rule has been moved to the first row in the table because it is more granular. Click **Save** to save your changes.

NAC Configuration: Defa	ult anage the end user connection experience and contr	ol network access based on aut	E3
Features Rules AAA: Default E-OPortal: Default	AAA Configuration: Default Authenticate Requests Locally for MAC Local Password Repository. Defau	(PAP), MAC (MsCHAP) *	
	Authentication Type User/MAC/Hos RADIUS Monitor A Any A	t Match Location Any Any	Authentication Methy Local Authentication Proxy RADIUS
	*		•
		Save	Close Help

10. Click the Enforce toolbar button to enforce the new configuration to your engine groups.

Any authentication request coming from an IP address that matches the list of RADIUS monitor clients will be authenticated using the password you provided in the AAA mapping. In these cases, the username does not matter. The password configured will not be able to be used for authentication from any other part of the network. The Extreme Access Control engine responds back with a basic accept to any RADIUS monitor client's RADIUS request.

Related Information

For information on related help topics:

• Engine Group Configuration Tab

Extreme Access Control Performance Tuning in Extreme Management Center

The following sections provide detailed information on how to use specific Extreme Access Control tools and features to monitor and improve Extreme Access Control performance.

- Monitoring Active End-Systems
- Tuning Data Persistence
- Tuning Extreme Access Control Capacity
- Using Extreme Access Control Distributed Cache

Monitoring Active End-Systems

Monitoring the total number of active end-systems on the network, as well as the number per engine, is useful in determining whether authentication load is distributed evenly between available Extreme Access Control engines. Some engines may be at or near capacity, while others may be underutilized and available to handle additional end-systems. Use this information to review your primary and secondary Extreme Access Control engines and the switches that authenticate against each engine, to determine whether adjustments can be made to more evenly distribute the load. The goal is to evenly distribute the authentication and captive portal load across all available Extreme Access Control engines as much as possible.

Engine capacity information also provides data points you can use for capacity planning and determining future hardware needs based on current load and expected growth, as well as targeting areas for design improvements such as implementing additional redundancy and disaster recovery.

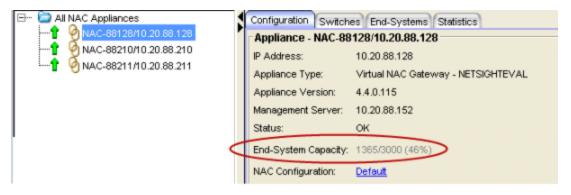
As you study the capacity information, keep in mind that an engine failure for any reason means that end-systems authenticating against that engine now authenticates against the designated backup engine. In an environment where there are two Extreme Access Control engines each responsible for authenticating 2,500 end-systems, a single engine outage can mean that all 5,000 end-systems might possibly authenticate against the one remaining engine. Depending on a variety of factors, oversubscribing an engine could lead to scenarios such as failed or intermittent authentication responses, poor enduser experience, or restricted access to the network.

NOTE: Any authentications previously performed by the unavailable primary engine remain authenticated until the session is removed or times out. At that point, subsequent authentication requests are sent to the backup engine. Whether authentication requests automatically revert to the primary engine once it is deemed available is a function of individual switch RADIUS operation.

Locating the End-System and Capacity Information

The **Configuration** tab in NAC Manager displays authenticated end-system and capacity information for each Extreme Access Control engine. To view this information, select an Extreme Access Control engine in the NAC Manager tree and then select the **Configuration** tab. The Current Capacity field indicates the number of end-systems that have authenticated to the Extreme Access Control engine within the last 24 hours out of the total supported authentication capacity for the Extreme Access Control engine. For example, a current capacity value of 1365/3000 indicates that 1,365 end-systems have authenticated against this Extreme Access Control engine within the last 24 hours of engine within the last 24 hours of authenticated against this Extreme Access Control engine within the last 24 hours, and this specific engine is rated to handle 3,000 authentications. The total number of supported authentications may vary depending on enginetype.

Configuration Tab - Current Capacity



To view capacity information for all Extreme Access Control engines in one place, select the All NAC Appliances folder in the tree and click on the NAC Appliances tab. The authenticated user counts and engine capacity are displayed under the Capacity column.

NAC Appliances Tab - Capacity

B- AI NAC Applences	Welcome Configuration	Switches End-Syste	ms NAC Appliances	Statistics								\frown
-1 NAC-88210/10 20.88 210	Name	IP Address	Appliance Type	Primary Count	Secondary Count	Model	Version	CPU Load (0-100%)	Memory Used	Memory Available	Connected Agents	Capacity
	NAC-88128	10.20.88.128	NAC Gateway	1	0	NETSIGHTEVAL	4.4.0.115	0	431.48 MB	11.22 GB	0	744/3000 (25%)
	NAC-88211	10.20.88.211	NAC Gateway	2	1	NETSIGHTEVAL	5.0.0.160B	0	8.82 GB	2.91 GB	0	1365/3000 (46%)
1	NAC-88210	10.20.88.210	NAC Gateway	0	2	NETSIGHTEVAL	5.0.0.153B	0	663.85 MB	10.99 GB	0	79/3000 (3%)

Engine load reporting is also available within Extreme Management Center. The <u>NAC Appliance Load report</u> provides a summary of end-system usage for each Extreme Access Control engine on the network, including the number of active end-systems on the engine, and the number of authentication and captive portal requests per minute.

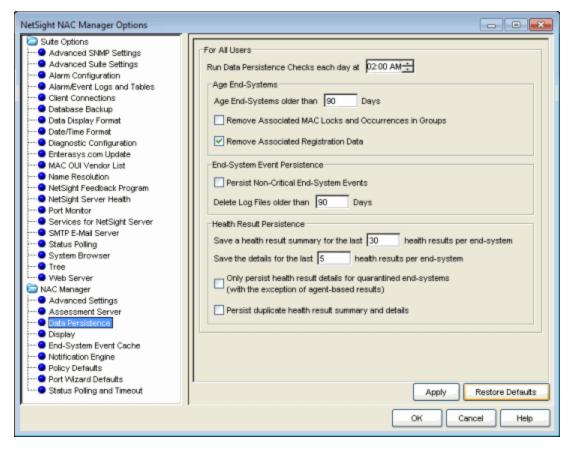
Tuning Data Persistence

NAC Manager Data Persistence options provide granular control for defining how long end-system and end-system related information is retained and stored. These options let you customize the aging of stale end-systems, as well as the length of time to retain end-system events and end-system assessment health results.

From the NAC Manager menu bar, select Tools > Options to open the Options window. Expand the NAC Manager Options folder and select Data Persistence. The options included in the three sections of the window are described below.

For more information on NAC Manager Data Persistence options, see the NAC Manager Options Window Help topic in the NAC Manager User Guide.

Data Persistence Options



Age End-Systems

Retaining large amounts of stale end-system data can lead to Extreme Management Center client performance issues as well as server performance degradation in larger networks or on Extreme Management Center servers that may not have optimal hardware. Reducing unnecessary stale data in the database leads to improved performance, smaller (and faster) backup files, as well as reduced disk utilization on the server. (Performance differences vary between individual Extreme Access Control deployments.)

By default, stale end-systems are aged out after 90 days of inactivity. In high volume networks with frequent short-term users (for example, an environment with a lot of visitors or contractors), it might be appropriate to change the number of days to a lower amount. Aging stale end-systems removes inactive and potentially one-time end-systems from the database and NAC Manager tables, making it easier to monitor and locate active end-systems on the network.

The option to remove associated MAC locks and occurrences in groups is disabled by default. For networks with a large volume of short-term authentications, as well as users who connect to the network infrequently but on a recurring basis, this ensures these end users retain any assigned end-system group membership and are authorized against the proper Extreme Access Control rule the next time they authenticate to the network, should their endsystem age out. If this is not a concern, you may consider selecting this option to remove group membership. Excessively large end-system groups can have an impact on both the server and engine. This varies by deployment, but generally, networks containing end-system groups with 30,000 to 35,000 end-systems should have this option selected to ensure stale data is properly handled.

By default, end-system registration data associated with stale end-systems is also removed when an end-system ages out. Even though registrations have an independent expiration timer and removal option, this removes registrations associated with stale end-systems prior to the defined registration expiration, maintaining active end-system registrations in the database and keeping endsystem and registration information in sync.

End-System Event Persistence

End-system events track authentication and Extreme Access Control related activity such as IP and OS resolution, state changes, and assessment information. These events are maintained in memory and are archived in log files on the Extreme Management Center server. Due to the high volume of event activity, the option to persist non-critical events is disabled by default, and certain non-critical end-system events are not retained. (Examples of noncritical events include duplicate or unchanging events, such as events tied to reauthentication where an end-system's state hasn't changed.) Removing events that are redundant or show no change leaves more space to retain those events that do indicate active changes, maintaining end-system event efficiency.

However, networks with fewer end-systems, or those not utilizing Extreme Access Control features that create additional events such as registration and assessment, could choose to enable the option to persist non-critical events, since they can display events maintained in memory for a longer period than those in a more dynamic environment.

End-system events are stored in log files on the Extreme Management Center server. These logs are available in the <install directory>/Extreme_ Networks/NetSight/appdata/logs directory and are identified by the filename convention: nacESE.date_version.log (for example, nacESE.2012_12_31_01.log, nacESE.2012_12_31_02.log). Events are continuously saved in the nacESE files with each individual file growing to about 5 MB before it is archived and a new log file is started for that day. Each day, when the Data Persistence check runs, it removes all log files that are older than the number of days specified (90 days by default). The length of time to retain the log files depends on your security policy (how long records need to be kept), system hardware limitations (disk availability), and the overall amount and type of activity logged.

The number of end-systems and activity on the network directly impacts the number of nacESE event log files generated on a daily basis. Monitoring the number of files generated for a period of time provides a baseline of the amount of space being consumed by these events and helps determine whether additional action may be required to manage them.

Health Result Persistence

By default, a health result summary is saved for the last 30 assessments per endsystem. A full, detailed health result report is retained for the last five assessments for each individual end-system. The number of summaries and detailed reports to save depends on your company's security policy, and how long summary and detailed assessment data is required.

For example, in an environment where end-systems are managed and generally compliant, retaining extended detailed assessment results may not be necessary. Whereas, in some environments, end-system monitoring is much more stringent and specific guidelines specify the length of time this type of data must be retained. Other factors to consider when reviewing these settings are the frequency, level (heavy versus light), and type of scans (agent-less or agent-based) being performed.

If you select the option to only save health result details for quarantined endsystems, all health result details resulting in an Accept State are discarded. This applies only to agent-less assessment, as agent-based health result details are always saved for all end-systems, regardless of whether the result indicates an Accept or Quarantine state. (The number of health result details saved is determined by the option described above.)

You can select an option to save duplicate health result summaries and details, if desired. By default, duplicate health results are not saved. For example, if an end-system is scanned five times during the week with identical assessment

results each time, the duplicate health results are not saved (with the exception of administrative scan requests such as Force Reauth and Scan, which are always saved). This reduces the number of health results saved to the database.

Tuning Extreme Access Control Capacity

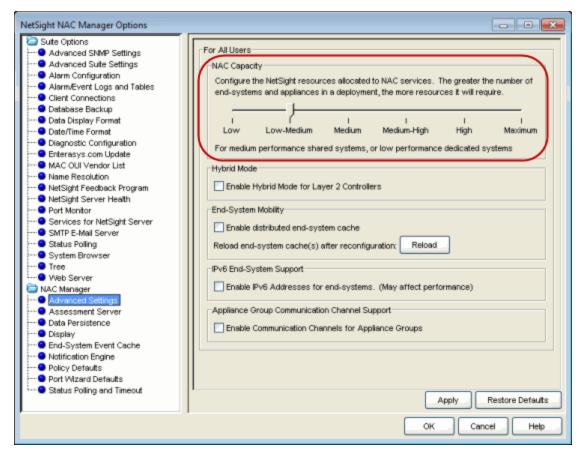
The NAC Capacity option in NAC Manager controls the configuration of internal Extreme Management Center resources (server processing queues, timing, etc.) allocated to Extreme Access Control services. These resources are specifically targeted towards the processing of incoming end-systems, end-system events, and health result data sent from Extreme Access Control engines to the server. The greater the number of end-systems and engines in your Extreme Access Control deployment, the more resources Extreme Access Control services require for processing the incoming information updates sent by each Extreme Access Control engine.

Indications that capacity settings may be insufficient can surface in the form of slower processing of end-system information or possibly missing updates. Modifying the capacity level upwards, incrementally allocates additional server resources dedicated to the processing of this data. Each level provides increased queue sizes to handle the greater volume of incoming data. In addition, changes are made in the frequency in which data is saved, as well as the amount of data saved in each operation. The changes allow Extreme Management Center to more efficiently process the larger amount of data.

If insufficient resources is not the actual problem, the allocation of additional resources may ultimately have little or no effect on performance. Because of this, it is important to first verify that the Extreme Management Center server is installed on a system with appropriate resources in terms of both hardware and role (a dedicated management server versus one performing multiple roles) and that the resources are commensurate with the size of the Extreme Access Control deployment.

Insufficient server hardware could appear as a Extreme Management Center performance issue, where in reality, the server hardware resources are not adequate for the deployment. Larger Extreme Access Control implementations with a high number of end-systems should consider a Linux-based operating system as additional resources such as memory can be allocated over and above Windows servers. To adjust Extreme Access Control Capacity, access the NAC Manager options. From the NAC Manager menu bar, select Tools > Options to open the Options window. Expand the NAC Manager Options folder and select Advanced Settings.





Using Extreme Access Control Distributed Cache

The NAC Manager distributed end-system cache is an optimization recommended for large enterprise environments as a way to improve response times when handling end-system mobility. Enabling this option improves Extreme Access Control performance when discovering new end-systems as they connect, or when end-systems move (and authenticate) from one location to another in the network.

Use of the distributed end-system cache feature requires that it is activated on both the Extreme Management Center server and on all Extreme Access Control

engines in order to take advantage of the optimized communications. (See the instructions below.)

NOTE: The Distributed end-system cache functionality must be enabled in environments using the Extreme Access Control DNS Proxy to redirect clients to the captive portal.

When this feature is enabled, end-system information similar to that in the endsystems table is stored in memory on the Extreme Management Center server and Extreme Access Control engine. Each cache contains the same up-to-date information, allowing the engine to perform lookups for end-system information in its local memory cache instead of having to query the server for updated information. Any changes to end-system information are propagated from each engine to the Extreme Management Center server, which then replicates updates to each Extreme Access Control engine so all have a synchronized copy of real time end-system information.

Implementation of this feature is **not** recommended unless there is sufficient network bandwidth available to handle the additional overhead in communicating updates, as well as a fast connection between the Extreme Management Center server and the Extreme Access Control engine. Additional consideration should be taken prior to implementing this functionality on engines that reside in a location where the data path traverses a WAN link.

To enable on the Extreme Management Center server:

From the NAC Manager menu bar, select Tools > Options to open the Options window. Expand the NAC Manager Options folder and select Advanced Settings. The option is in the End-System Mobility section. When you enable or disable this option, you must click the **Reload** button to reload the cache configuration on the Extreme Management Center server.

NetSight NAC Manager Options Suite Options For All Users Advanced SNMP Settings Advanced Suite Settings NAC Capacity Alarm Configuration Configure the NetSight resources allocated to NAC services. The greater the number of Alarm/Event Logs and Tables end-systems and appliances in a deployment, the more resources it will require Client Connections Database Backup Data Display Format 1 Medium-High High Low-Medium Medium Maximum Date/Time Format Low Diagnostic Configuration For medium performance shared systems, or low performance dedicated systems Enterasys.com Update MAC OUI Vendor List Hybrid Mode Name Resolution Enable Hybrid Mode for Layer 2 Controllers 🔍 NetSight Feedback Program NetSight Server Health Port Monitor End-System Mobility Services for NetSight Server Enable distributed end-system cache SMTP E-Mail Server Status Polling Reload end-system cache(s) after reconfiguration: Reload System Browser Tree IPv6 End-System Support Web Server Enable IPv6 Addresses for end-systems. (May affect performance) 🚞 NAC Manager Adva Appliance Group Communication Channel Support Assessment Server Data Persistence Enable Communication Channels for Appliance Groups Display End-System Event Cache Notification Engine Policy Defaults Port Wizard Defaults Status Polling and Timeout Apply Restore Defaults OK Cancel Help

Advanced Settings Options - End-System Mobility

To enable on the Extreme Access Control engine:

In the engine **Configuration** tab, click on the **Advanced Configuration** button. Enable the option in the NAC Appliance Advanced Configuration window. Enabling this option requires an enforce of the engine.

 NAC Appliance Groups All NAC Appliances 10.20.80.8/10.20.80.8 10.20.80.22/10.20.80.22 10.20.80.32/10.20.80.22 10.20.80.32/10.20.80.32 10.20.80.32/10.20.80.32 10.20.80.37/10.20.80.37 10.20.80.37/10.20.80.37 10.20.80.38/10.20.80.38 10.20.80.38/10.20.80.38 10.20.80.38/10.20.80.38 10.20.80.38/10.20.80.38 10.20.80.38/10.20.80.48 10.20.80.78/10.20.80.78 10.20.85.10/10.20.85.10 172.16.1.38/172.16.1.38 172.16.1.38/172.16.1.39 	Configuration Switches End-Systems Statistics Appliance - NACDEMO/10.20.88.101 IP Address: 10.20.88.101 Appliance Type: NAC Gateway - NAC-A-20-2 Appliance Version: 4.30.71 Management Server: 10.20.88.100 Status: OK Current Capacity: 0/3000 (0%) NAC Configuration: NetSight-NAC Lab NAC Configuration Interface Summary Interface: Interface: eth0 Management, Registration & Remediation IP: 10.20.88.101/24 Interface: eth1 Off NAC Appliance Advanced Configuration NAC Bypass Configuration Imagement State Configuration NAC Bypass will disable NU Enable distributed end-system cache
	NAC Bypass Configuration

Configuration Tab - Advanced Configuration

NAC Manager and Extreme Access Control Troubleshooting in Extreme Management Center

The following sections provide information on tools used when troubleshooting NAC Manager and Extreme Access Control engine issues.

- NAC Manager Event Logging
- Extreme Access Control Engine Real-time Status
- End-System Troubleshooting

NAC Manager Event Logging

The Event View at the bottom of the NAC Manager main window displays error and informational messages about NAC Manager operations and provides information on end-systems attempting to connect to the network through an Extreme Access Control engine.

NAC Manager Event View

NAC	Manager Events	End-Systems	Activity NAC Appliance Events	Audit Events		
S	 Acknowledge 	Severity	Category	Timestamp 2	Source	Subcomponent
689		😑 Info	Application	09/20/2012 11:43:14 AM		
690		🔵 Info	Application	09/20/2012 11:43:14 AM		
691		😑 Info	Configuration	09/20/2012 08:45:58 AM		
692		🔵 Info	Configuration	09/20/2012 08:45:58 AM		

There are four tabs:

• NAC Manager Events – This tab displays error and informational messages about NAC Manager system operations, including configuration changes and enforce operations.

Use this tab when trying to locate forensic information such as when and who made changes to the Extreme Access Control configuration, and when and for how long communication with an Extreme Access Control engine was lost. This event log also captures NAC Manager functional and security-related warnings that the system issues when auditing its own configuration, as well as events tied to <u>data persistence</u> checks, including which end-systems were removed and when.

Important system notification messages are also logged here, including when new agent-less assessment updates are available and when certain system default credentials should be changed.

- End-Systems Activity This tab provides information on all the end-systems that have attempted to connect to the network. It displays all end-system activity since the client was launched.
- NAC Appliance Events This tab provides information on Extreme Access Control engine system events including RADIUS configuration success or failure, completed reauthentications, and management logins (such as Telnet or SSH configured for external authentication). The event log displays engine activity since the NAC Manager client was launched and like NAC Manager Events, is an excellent source for historical information when performing a forensic investigation of a recent event.
- Audit Events This tab provides information on Extreme Access Control Registration events such as when a device or user is added during the registration process, or an end-system is added, removed, or updated via the registration administration web page. It displays all registration activity since the client was launched.

For more information, see the Event View Help topic in the NAC Manager user guide.

Extreme Access Control Engine Real-time Status

Use the following tools to monitor Extreme Access Control engine real-time statistics, as well as view diagnostic information in the Extreme Access Control engine Administration Web Page (WebView), and Extreme Access Control information in the Extreme Management Center **Administration** tab.

NAC Appliances Tab

The NAC Appliances tab provides CPU and memory utilization statistics for all your Extreme Access Control engines. The CPU Load column shows the percentage of the engine's CPU that is currently being used. This value gives you an indication of how busy the engine is and helps you determine if your network needs additional engines, or if you need to change your network configuration so that the load is more evenly distributed among your existing engines.

NAC Appliances Tab

Welcome End-Sys	stems NAC Appliance	83					
Name	IP Address	Appliance Type	Version	CPU Load (0-100%)	Memory Used	Memory Available	Capacity
10.20.80.39	10.20.80.39	NAC Gateway	4.2.0.DEV	0	0.0 B	0.0 B	0/1500 (0%)
10.20.80.38	10.20.80.38	NAC Gateway	4.4.0.DEV	0	0.0 B	0.0 B	0/3000 (0%)
10.20.80.37	10.20.80.37	NAC Gateway	4.4.0.DEV	0	496.39 MB	11.39 GB	0/3000 (0%)
172.16.1.39	172.16.1.39	NAC Gateway	NAC-V v4.3.0.demo	0	0.0 B	0.0 B	

In addition to the information in the table, you can launch two FlexViews with CPU, memory, and disk utilization information from the right-click menu off one or more engine in the **NAC Appliances** tab.

Launch the CPU Utilization View (Host Processor Load FlexView).

	or Load									
M -	Flex/View: Host Pr	ocessor Load	-	• • • • ≥		Poll Freque	incy: 0	-		¥1
IP Addre	ess 94 Device Inde	x \$\$		Description				1 Mir	nute Processo	r Loa
0.20.80.28	768	GenuineIntet	Intel(R) Xeo	on(R) CPU	E5410	@ 2.33GHz	1			
20.80.28	769	GenuineIntet	Intel(R) Xeo	on(R) CPU		@ 2.33GHz	1			
0.20.80.28	770	GenuineIntet		17		@ 2.33GHz	1			
20.80.28	771	GenuineIntet		1.7		@ 2.33GHz	1			
0.20.80.38	768			tium(R) D CPU 3			1			
0.20.80.38	769	GenuineIntel:	Intel(R) Pen	tium(R) D CPU 3	3.20GHz		1			

Host Processor Load FlexView

Launch the Memory and Diskspace Utilization View (Host Storage FlexView).

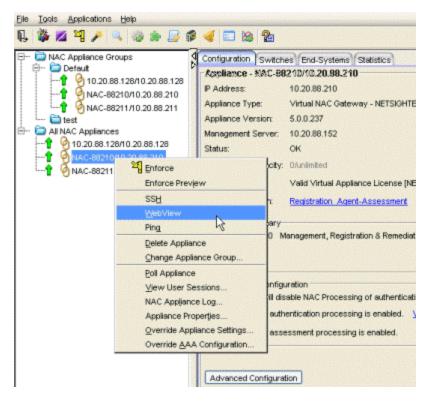
FlexView:	- Host Storage		Poll Pre	squency: 0	
IP Address 9.	L Type	Description	Percent Used	Total Memory	Memory Used
0.20.80.28	hrStorageRam	Physical memory	37.85%	8.5 GB	3.22 GB
0.20.80.28	hrStorageVirtualMemory	Virtual memory	15.04%	21.39 GB	3.22 GB
0.20.80.28	hrStorageOther	Memory buffers	3.73%	8.5 GB	317.27 MB
0.20.80.28	hrStorageOther	Cached memory	100%	2.34 GB	2.34 GB
0.20.80.28	hrStorageVirtualMemory	Swap space	0%	12.89 GB	0 B
0.20.80.28	hrStorageFixedDisk	1	2.51%	50.4 GB	1.27 GB
0.20.80.28	hrStorageFixedDisk	/opt	1.27%	167.77 GB	2.13 GB
0.20.80.38	hrStorageRam	Physical memory	95.02%	1.05 GB	1 GB
0.20.80.38	hrStorageVirtualMemory	Virtual memory	31.11%	3.22 GB	1 GB
0.20.80.38	hrStorageOther	Memory buffers	-	289.73 MB	
0.20.80.38	hrStorageOther	Cached memory	-	432.89 MB	-
0.20.80.38	hrStorageOther	Shared memory	-	0 B	
0.20.80.38	hrStorageVirtualMemory	Swap space	0%	2.16 GB	40.96 KB
0.20.80.38	hrStorageFixedDisk	1	6.1%	16.14 GB	983.52 MB
0.20.80.38	hrStorageFixedDisk	/opt	3.85%	41.27 GB	1.59 GB

Host Storage FlexView

Extreme Access ControlEngine Administration Web Page (WebView)

To access status and diagnostic information for an individual Extreme Access Control engine, launch WebView by right-clicking on an Extreme Access Control engine in the left-panel tree, as shown below. (You can also access the administration web page using the following URL: https://<Extreme Access ControlengineIP>:8444/Admin.)

The default user name and password for access to this web page is "admin/Extreme@pp." The username and password can be changed in NAC Manager using the Advanced Configuration window (available from the Tools menu > Manage Advanced Configurations) and selecting the Engine Settings > Miscellaneous Tab > Web Service Credentials field. Launch WebView



The Home web page provides resource details such as current CPU and memory usage. Status details provide a Current and Maximum counter for many critical functions. Excessive authentication requests or failures are easily identified, including when the Max Reached value occurred. This helps to identify the severity of a current problem or match information with prior events when performing a forensic review.

NOTES: Memory usage is normally close to 100% to allow for better performance.

Engine Administration Web Page

44

4 🤐 Home
E Home
⊳ 📴 <u>Status</u>
Diagnostics

- Þ 📴 Log Files
- Downloads

Difference

Configuration Details

NAC Engine InformationNAC Gateway - NETSIGHTEVAL v.5.0.0.237License StatusValid License [NETSIGHTEVAL]NAC Engine IP10.20.88.210NetSight Server IP Address10.20.88.152NAC Server Statusup, ready since Thu Sep 05 15:13:23 EDT 2013NAC Up Time (HH:MM:S5.mmmr)250:23:03.356		
NAC Engine IP 10.20.88.210 NetSight Server IP Address 10.20.88.152 NAC Server Status up, ready since Thu Sep 05 15:13:23 EDT 2013	NAC Engine Information	NAC Gateway - NETSIGHTEVAL v.5.0.0.237
NetSight Server IP Address 10.20.88.152 NAC Server Status up, ready since Thu Sep 05 15:13:23 EDT 2013	License Status	Valid License [NETSIGHTEVAL]
NAC Server Status up, ready since Thu Sep 05 15:13:23 EDT 2013	NAC Engine IP	10.20.88.210
	NetSight Server IP Address	10.20.88.152
NAC Up Time (HH:MM:55.mmmm) 250:23:03.356	NAC Server Status	up, ready since Thu Sep 05 15:13:23 EDT 2013
	NAC Up Time (HH:MM:S5.mmmm)	250:23:03.356

Resource Details

CPU Usage	User=0.12% System=0.01% Niced=0.00% Idle=99.87% Total=0.13%
Memory Usage	Used=13.79% Free=86.21% Total=11.64 GB
Swap Space	Used=0.00% Free=100.00% Total=11.64 GB
NAC Process	Heap=68.33% Non-Heap=31.67% Total=139.58 MB

Status Details

Statistic	Current	Maximum	Total	Max Reached
Authentication Requests	0/min	195/min	34	Thu Sep 05 15:14:32 EDT 2013
Authentication Successes	0/min	2/min	0	Thu Sep 05 15:14:32 EDT 2013
Authentication Failures	0/min	3/min	0	Thu Sep 12 15:24:05 EDT 2013
Radius Challenges	0/min	9/min	0	Mon Sep 09 18:43:52 EDT 2013
Invalid Authentication Requests	0/min	4/min	34	Thu Sep 12 17:31:05 EDT 2013
Duplicate Authentication Requests	0/min	0/min	0	Not Available
Malformed Authentication Requests	0/min	1/min	0	Thu Sep 05 15:14:32 EDT 2013
Bad Authentication Requests	0/min	0/min	0	Not Available
Dropped Radius Packets	0/min	193/min	0	Thu Sep 05 15:15:32 EDT 2013
Unknown Radius Types	0/min	0/min	0	Not Available
Assessment Requests	0/min	2/min	24	Sat Sep 07 13:39:41 EDT 2013
Captive Portal Requests	0/min	2/min	8	Mon Sep 09 12:31:51 EDT 2013
Contact Lost Switches	0/min	0/min		Not Available
IP Resolution Failures	0/min	0/min	0	Not Available

For more information, see the Extreme Access Control Engine Administration Web Page section of the Extreme Access Control Deployment Guide, which is in the NAC Manager user guide.

Extreme Access Control Switches and Routers

When troubleshooting issues involving authentication, IP resolution, and reauthentication (etc.), the Switches & Routers page within WebView provides a variety of useful real-time data.

At the top, current and historical information is displayed on a per-switch basis. This provides insight into problems such as a single switch flooding the network with authentication requests, as well as comparative data that can be used to spot abnormalities such as a switch with a limited number of active end-systems showing an excessive number of authentications over the last month.

Toggle Link: ifAdminStatus MIB (0) Cisco dot1xPaePort & Toggle Link (0)

Cisco dot1xPaePort & Toggle Link (0)

The Switch Configuration section is an overview of all switches assigned to the Extreme Access Control engine, the RADIUS response attributes they are configured for, and the SNMP credential the Extreme Access Control engine is using to communicate with the switch. This information can be used to identify whether the Extreme Access Control engine is using the current SNMP credentials to contact the switch. This can be confirmed under the Switch Dynamic Information where SNMP Contact will show as Contact Lost.

More critical information here, although perhaps more useful for support technicians, are the various workers assigned to each switch. These are dictated through the switch discovery process and detail how the Extreme Access Control engine performs various functions such as using RFC 3576 or Toggle Link for reauthentication of an end-system. The SNMP Contact is from the perspective of the Extreme Access Control engine to the switch, which may be different than from Extreme Management Center Console to the switch.

Engine Administration Web Page

Established

10.20.88.210 Clear

10.20.88.220

10.20.88.221

Switch IP	Total	Minute:	Current (Min/Max)	Hour: Current (Min/	Max) Day: Curren	t (Min/Max) Las	t 31 Days			
0.20.80.125	77		0(0/3)		0/21)	0(0/68)	77			
0.20.80.126	0		0(0/0)		(0/0)	0(0/0)	0			
0.20.82.3	1083		0(0/1)			06 (266 / 298)	1083			
0.20.88.196	0		0(0/0)		(0/0)	0(0/0)	0			
0.20.88.210	0		0(0/0)		(0/0)	0(0/0)	0			
0.20.88.220	0		0(0/0) 0(0/0)		(0/0) (0/0)	0(0/0)	0			
				(7)						
witch (Switch IP	Type	juratio	n Information Primary RADIUS	(7) Secondary RADIUS	RADIUS Response	Attributes	SNMP Credentials	s Device Lock	SNMP Lock	
0.20.80.125	Laver 2	Dut-DF-Band	10.20.88.211	N/A	Enteras	ys Policy	Dev AuthPriv	Not Locked	SNMP Semaph	ore, permits: 10, gueued requests: 0
0.20.80.126	Layer 2	Dut-DF-Band	10.20.88.211	N/A	RFC 3580 - VLAN ID & En	terasys (HiPath) Wirele	s Dev AuthPriv	Not Locked	SNMP Semaph	ore, permits: 5, queued requests: 0
10.20.82.3	Layer 21	Dut-Df-Band	10.20.88.211	N/A		- VLAN ID	Dev-v1	Not Locked		ore, permits: 5, queued requests: 0
0.20.88.196		Dut-Df-Band	10.20.88.211	N/A		Path) Wireless	Dev-v1_priv	Not Locked	SMMP Semaph	ore, permits: 10, queued requests: 0
0.20.88.210		Dut-Of-Band	10.20.88.211	N/A		ys Policy	Dev_AuthPriv	Not Locked		ore, permits: 5, queued requests: 0
0.20.00.220		Dut-Of-Band	10.20.88.211	10.20.88.210		ys Policy	public_v1	Not Locked	SNMP Semaph	ore, permits: 5, queued requests: 0
0.20.88.221	Layer 2	Dut-Of-Band	10.20.88.211	N/A	RFC 3580	- VLAN ID	Cisco3750_AuthNoPriv	Not Locked	SNMP Semaph	ore, permits: 5, queued requests: 0
witch I Switch IP	Dynar _{Cache}		ormation (7) Current SNMP Contac	t SNMP Failures	SvsObjectID	Firmware Versio	n Base MAC	RADIUS Worker		Re-authentication Worker
0.20.80.125			stablished	a and a followed	1.3.6.1.4.1.5624.2.1.129	8.11.2.2	00-1F-45-FC-CE-08	Enterasys Unencrypti		Enterasys MultiAuth MIDs (79)
0.20.00.153	Clear		stablished							
					1.3.6.1.4.1.5624.2.1.96	6.61.8.13	00-11-88-84-88-40	Enterasys Unencrypti	ed RADIUS MIB	Enterasys MultiAuth MIBs (0)
	Clear									
	Clear		stablished	0	1.3.5.1.4.1.9.1.516	12.2	00-14-F2-DC-88-C2	N/A		Cisco Authentication Framework(802.1x & M
0.20.80.126 0.20.82.3 0.20.80.196	And in case of the local division of the loc			0	1.3.6.1.4.1.9.1.516 1.3.6.1.4.1.4329.15.1.1.13	12.2 8.31.2.5	00-14-F2-DC-88-C2 00-0C-29-50-C4-7F	N/A Enterasys HiPath RAD		Cisco Authentication Framework(802.1x & M RFC 3576/5176 - Enterasys (HPath) Wireless

Extreme Management Center Administration - Identity and Access

0 1.3.6.1.4.1.5624.2.1.153 5.0.0.237

12.2

1.3.6.1.4.1.9.1.516

0 1.3.6.1.4.1.9.1.516 12.2

00-0C-29-DB-5A-9C N/A

00-21-1C-CD-E5-41 N/A

00-21-D7-80-3D-C1

The Administration tab in Extreme Management Center has an Identity and Access section that provides detailed diagnostic and statistical information pertaining to advanced Extreme Access Control functions. Information on web service calls, events, and distributed cache can be reviewed for signs of unexpected or failing processes.

Most of the information is useful to Engineering and Support technicians. More information is available under System-Wide Extreme Management Center Server Diagnostics in the Extreme Management Center Troubleshooting section of the Extreme Management Center Technical Reference.

Administration Tab

Diagnostics Scheduler	NAC Engine Status	
	NAC Engne Status	
Level: Diagnostic * Diagnostic Actions *	2" Refresh	
System Flows Historical Statistic Collector Identity and Access Distributed Cache Event Cache Event Datails Event Datails Event Results	NAC Engine Statistics Named List Updates: : 24 Named List Saves: : 17 Named List Resyncs: : 27 Total Registrations Aged : 1 Total End-Systems Aged : 0 Total Health Results Aged : 0 Named List Virite Count/Requests : 22 / 27 Named List Agy Write Time : 00:00:00.005 Named List Longest Write : Fri Sep 13 11:30:31 EDT 2013 Appliance Updater Queue Size : 0 Applance Updater Queue Peak : 1	
NAC Engine Status	Appliance Updater Queue Peak Time : Fri Sep 13 12:09:52 EDT 2013	
 NAC Web Service Counters Server Wireless 	Appliance Named List Resyncs : 10 Web Service Cal Failures : 0 Last Web Service Failure Time : Last Web Service Failure Message : Appliance 10.20.88.210	
5 Support	Applance Updater Queue Size : 0 Applance Updater Queue Peak : 1 Applance Updater Queue Peak Time : Fri Sep 13 12:09:52 EDT 2013 Applance Named List Resyncs : 10 Web Service Call Falures : 0 Last Web Service Falure Time : Last Web Service Falure Message :	
	Appliance 10.20.88.211 Appliance Updater Queue Size : 0 Appliance Updater Queue Peak : 1 Appliance Updater Queue Peak Time : Fri Sep 13 12:09:52 EDT 2013 Appliance Named List Resyncs : 7 Web Service Failures : 0 Last Web Service Failure Message :	

Extreme Access Control Status

The NAC Status option (previously available from the **NAC Appliances** tab) has been updated and replaced by the Extreme Management Center Show Support functionality described in the Extreme Management Center Troubleshooting section of the Extreme Management Center Technical Reference.

The nacstatus command is still available from the Extreme Access Control engine CLI and can be executed to provide detailed data regarding the Extreme Access Control engine. However, the Show Support function is the recommended data collection vehicle, as it provides a comprehensive look into both the operation of the server as well as all active Extreme Access Control engines.

End-System Troubleshooting

Use the following tools to monitor and trouble-shoot end-system issues in NAC Manager.

End-System Events in NAC Manager

Troubleshooting specific end-system issues starts with end-system events. Events provide time-stamped logs of when specific events occurred. It is helpful to correlate these events with diagnostic log data.

NAC Manager End-Systems Tab

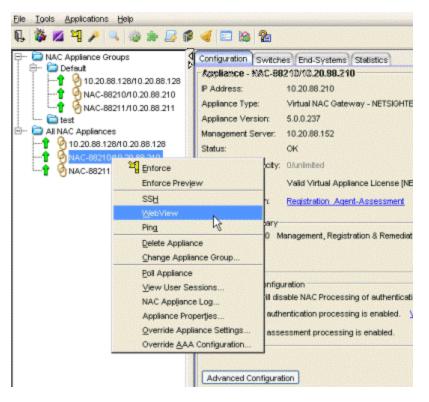
• 🔑	 MAC Address 	MAC OUI Vendor	IP Address	Switch IP	Switch Por	t	Actions	4
1	SIEMENS ENTERPRISE	Siemens Enterprise Commun			ge.1.18	^	Force	Dece #h
2	APPLE, INC:01:07:59	Apple, Inc.			maand-5s-ap2 (00-	1F-45	Forces	reautri
3	APPLE, INC:01:07:07	Apple, Inc.			ge.1.9		Force Reau	th and Scar
4	APPLE, INC:01:01:63	Apple, Inc	Apple, Inc maand-1n-ap1 (00-1F-45				Add to Group	
5	APPLE, INC:01:03:65	Apple, Inc. fe.5.17						
6	SAMSUNG ELECTRON	Samsung Electronics Co.,Ltd maand-4s-ap9 (maand-4s-ap9 (00-	1F-45	AC	
7	HTC CORPORATION 0	HTC Corporation				1F-45	Port M	ontor
8	APPLE, INC:01:02:63	Apple, Inc			GigabitEthernet1/0/	18 💌		mary
	for End-System: HTC COP	ult Summaries Health Result Del PORATION:01:06:30, through 09						
_	Time Stamp 👬	IP Address Switc					ste	U
0402	2012 03:40:25 PM	P	maand-1	n-ap1 (00-1F-45-68	-57-60):Prod Guest	Accept		Kenya Cop

Engine End-System Diagnostics

To access end-system diagnostic information for a specific Extreme Access Control engine, launch the Extreme Access Control engine administration web page by right-clicking on an Extreme Access Control engine in the left-panel tree and selecting WebView, as shown below. (You can also access the administration web page using the following URL: https://<Extreme Access ControlengineIP>:8444/Admin.)

The default user name and password for access to this web page is "admin/Extreme@pp." The username and password can be changed in NAC Manager using the Advanced Configuration window (available from the Tools menu > Manage Advanced Configurations) and selecting the Engine Settings > Miscellaneous Tab > Web Service Credentials field.

Launch WebView



Expand the Diagnostics folder and select End System Diagnostics. Enable diagnostics for both MAC and IP address.

Targeting diagnostics for a specific end-system enables a majority of the debug diagnostics available on a global level, but only for the specific end-system. Therefore, diagnostics can be enabled for an extended period of time without the concern of generating the excessive log files that are possible when global diagnostics are enabled.

The log data is saved to the same location as the global diagnostics, in the /var/log/tag.log file of the Extreme Access Control engine. A log entry is made in the tag.log helping to locate the portion of the log from which to start a review.

2013-09-13 14:51:20,783 INFO [ESD] Enabling verbose diagnostics for MAC: 00-18-8B-D6-E6-0C

2013-09-13 14:51:38,195 INFO [ESD] Enabling verbose diagnostics for IP: 10.20.87.100

Engine End-System Diagnostics

Contraction of the second seco	End System Diagnostics Configue Controls the diagnostics for specified end		
Status Jiagnostics	Lookup Data by MAC Address	Lookup Data by IP	Address
E Appliance/Server Diagnostics	Lookup		Lookup
Certificate Diagnostics			
Communication Diagnostics			
E Distributed Cache Diagnostics			
End-System Cache Diagnostic	End System Diagnostics by MAC Address	End System Diagr	nostics by IP Address
End System Diagnostics	00:18:8B:D6:E6:0C Verbose -	10.20.87.100	Verbose -
E Performance Diagnostics	Enable	Enable	
Þ 📴 Log Files			
Downloads			
D Utilities			

End-System Diagnostic Information

There are a variety of end-system troubleshooting tools available in NAC Manager by right-clicking on an end-system.

Launch End-System Diagnostic Tools

, 🔯 🖄 🏹 🔎 🔍 🕸 😹 🎜 🍕	🖾 😫 🔁										
Defaut	iguration Switch	hes End-Sy	stems Stat	tistics							
	End-Systems Find what: End Find in: All column					Options					
	MAC A	vidress	MAC	OUI Vendor		I P	Address	Swite	ch IP		
🗀 test 1	00:D0:59.A			ROSYSTEMS		10.20		10.20.82.3			
- Al NAC Appliances 2	00:16:86-54	005000 0 X500 0054 7 X		10.20.87.210		10.20.80.125					
	7C:61:93	Find			10.20.82.230		82.230	10.20.88.196			
🕈 🧑 NAC-88210/10.20.88.210 4	F0:A2:2	Filter			10.20.82.230		82.230	10.20.88.196			
	CC:3A:6	Sort			CH	10.20	82.230	10.20.88.1	96		
6	7C:C5:31	Auto Export			10.20.82.231		10.20.88.196				
7	7 00:26:08	Force Reauthentication			10.20.82.230			10.20.88.196			
8	5C:0A:5I		2010.02170150		CH	10.20	82.230	10.20.88.1	96		
9	00:1B:77		uthentication	and Scan	_			10.20.88.1			
	10 90:84:00	Assess End-System		100000	10.20.		10.20.88.1	96			
	2 4 4	Request A	gent Log File								
	7	Add to Gro	цρ					Service States	1/10/5		
End	I-System Ever	Lock MAC View Selected			suit Details 8. 2013 07:57:46						
Eve	ents for End-S										
	er on:	Edit Custom Information Clear Custom Information Delete End-Systems Configuration Evaluation Tool		Al columns +			Options	X			
	ar one l			2000			-				
	EN Dek EN Con EN Port EN Port			ity Extended State							
					Parah ing ID 6 dikeas						
				Resolving IP Address							
		Port Monito	r		Resolving IP Address Resolving IP Address		1				
		PortView	STREET STREET	1							
		Telnet to S	witch					10/2/2			
111			10000005050					-			
		SSH to Sw									
		Ping End-System			286			Renders State	6933		
▽		Select All			-				and the Arrest		
AC Manager Events End-Systems Activity NAC App	Contract Contractor	Table Tools			1	92253	Care and the				

- Configuration Evaluation Tool Test the rules defined in your NAC Configuration in order to determine what behavior an end-system will encounter when it is authenticated on an Extreme Access Control engine.
- **Port Monitor** View detailed port and switch status information for the selected endsystem including: information from interface statistics, CoS and authentication information, the Reauth Interval and Quiet Period, the interface PVID, and errors on the port.
- **PortView** View a variety of detailed port information and statistics presented in a network topology view. PortView displays the end-system in a graphical view based on how it connects to the network. From here, tabs are available that provide interface statistics, switch resource data, detailed Extreme Access Control end-system information, as well as flow data, if enabled. A right-click on the switch opens menu options to drill into more specific switch-related data. For wireless end-systems, a Real Capture can be launched from this view providing real-time packet capture of end-system communications.

- Telnet to Switch Launches a Telnet session to the switch the end-system is connected to.
- SSH to Switch Launches a Secure Shell (SSH) session to the switch the end-system is connected to.
- **Ping End-System** Open a window where you can ping the end-system to determine if it can be contacted. You can view the results of the ping in the log in the window. You can also click Clear to enter another IP address or host name, if you wish.

3/2018 8.1 Revision -00 Contents Subject to Change Without Notice