Monitor 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 Access Control health. These reports provide you with the information you need to monitor, analyze, and troubleshoot Access Control problems.

Monitor Access Control Engine Performance

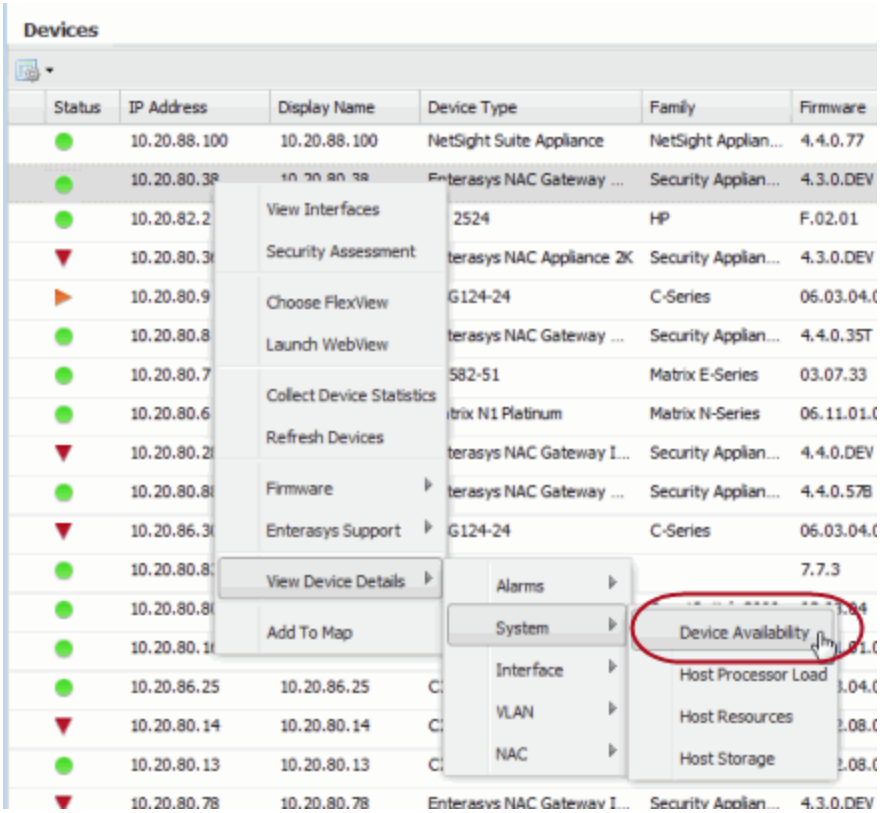
The Access Control engine Device Availability report provides a historical overview of the engine status. The report shows at-a-glance when an engine is offline, or whether an engine is consistently on and offline over time. The report lets you quickly determine the specific date when an engine is unavailable 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 Access Control engine logs for the dates in question (see Access Control Engine Log Locations), to gain additional insight into the possible root cause of the problem.

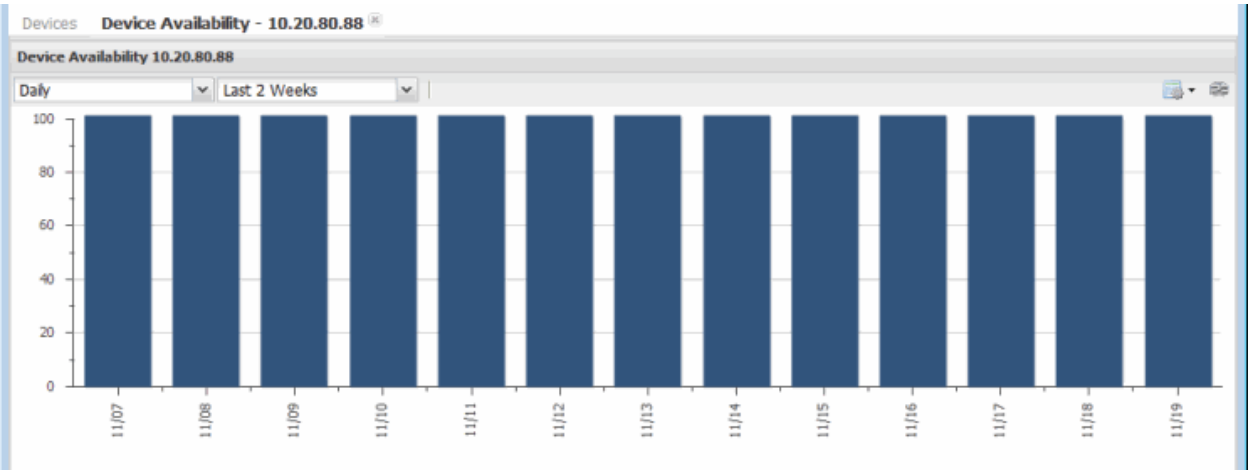
Access the Device Availability report from the **Network** tab. Right-click on an Access Control engine and select View Device Details > System > Device Availability, as shown here.

Accessing the Device Availability Report



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

Device Availability Report



Monitor Access Control Engine Memory Use

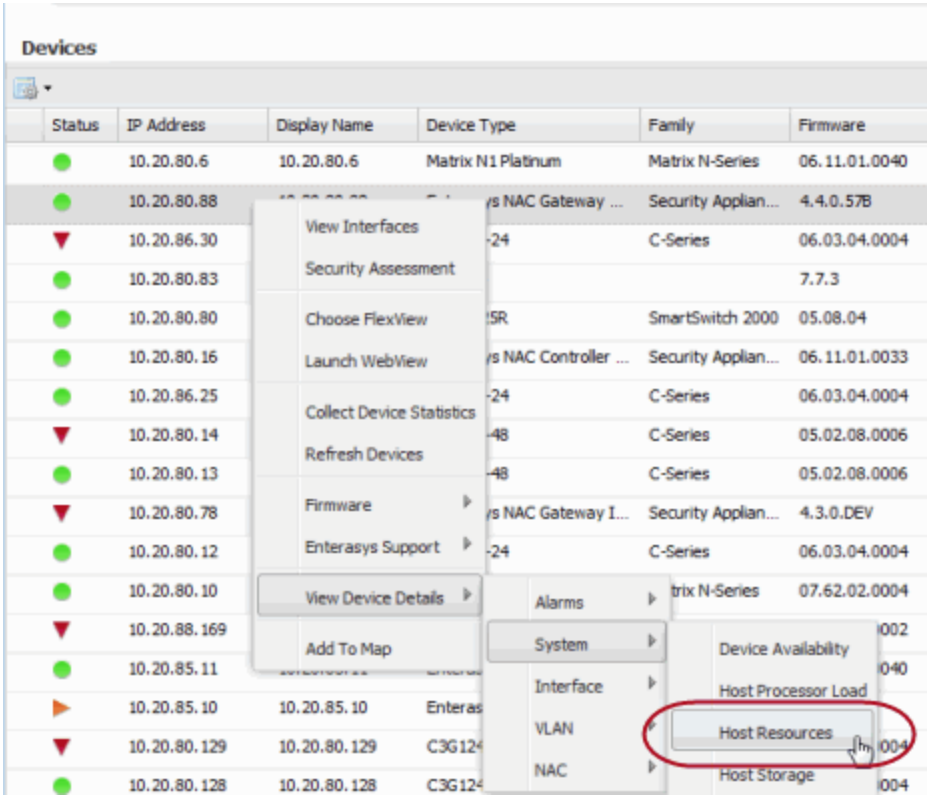
The Extreme Management Center Host Resources report lets you monitor physical, virtual, and swap memory usage on an Access Control engine.

As you monitor an engine's physical and virtual memory, keep in mind that it is common for Linux-based systems (such as the 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 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 Linux "top" Command 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.

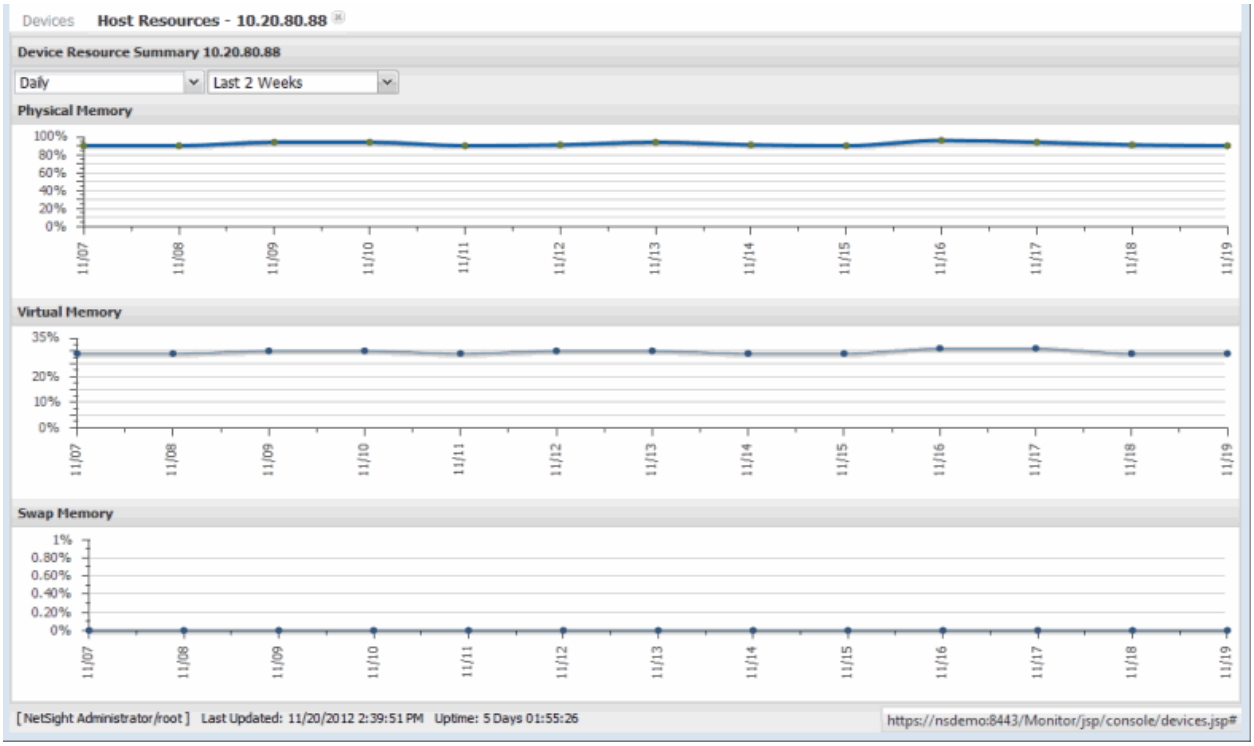
Use the **Network** tab to access the Host Resources report for an Access Control engine. Right-click on an Access Control engine and select View Device Details > System > Host Resources, as shown here.

Accessing the Host Resources Report



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

Host Resources Report

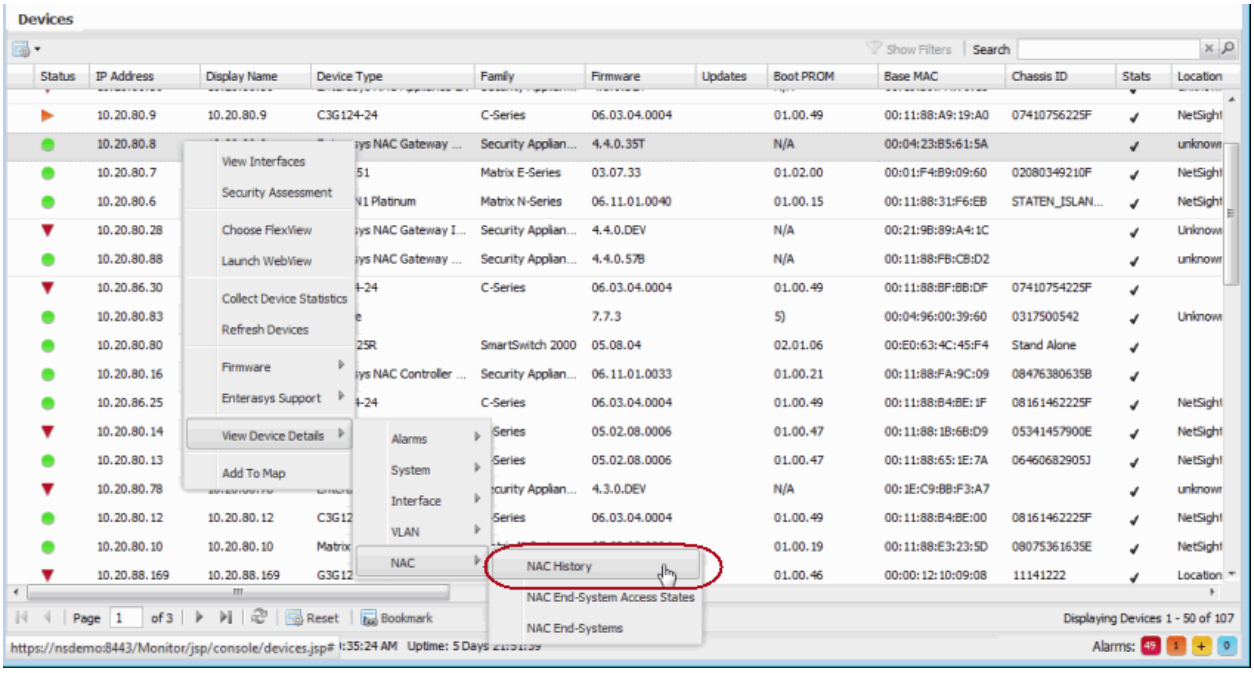


View Access Control Engine Historical Data

The NAC History report provides a detailed view of the overall Access Control engine load based on critical 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 Access Control Engine Load report, which presents current load data for all engines.

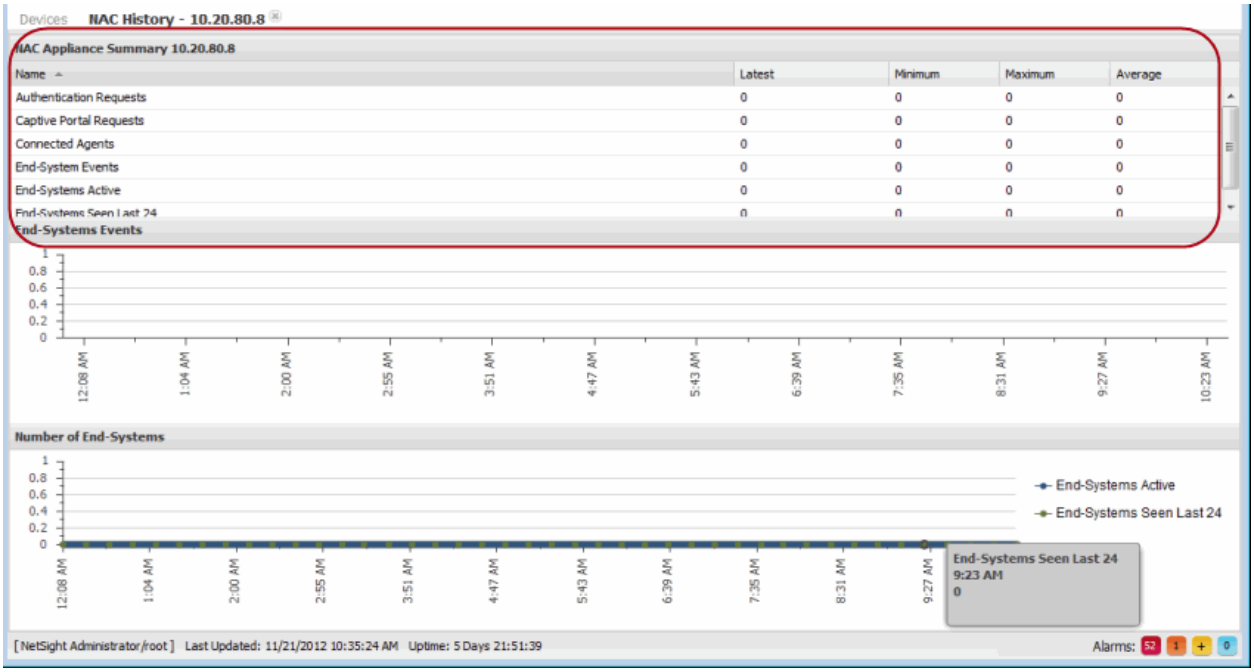
In Extreme Management Center, select the **Network** tab. Right-click on an Access Control engine and select View Device Details > NAC > NAC History, as shown here.

Accessing the NAC History Report



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

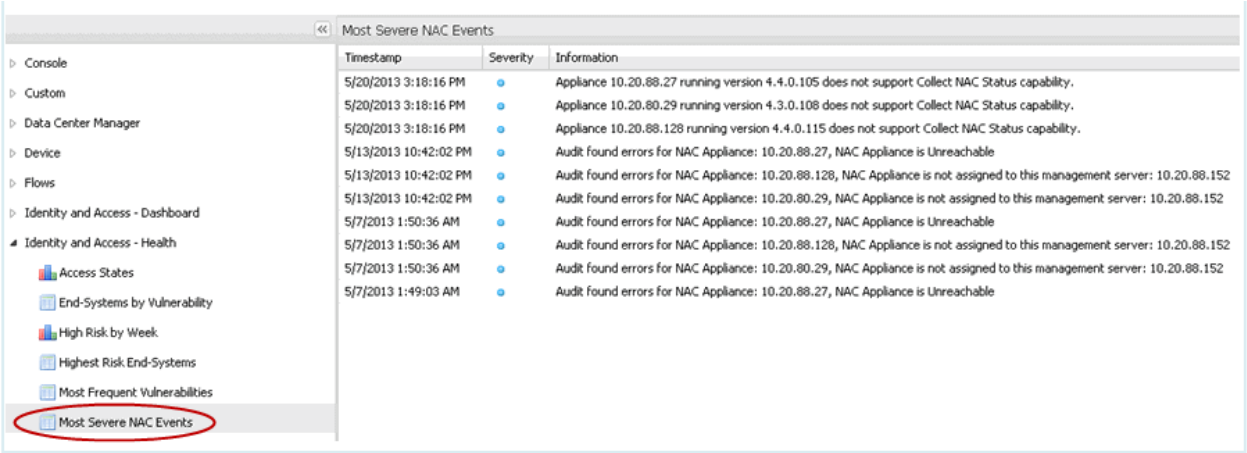


Monitor Access Control Critical Events

The Access Control report on Most Severe Access Control Events displays the 10 most severe 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 Technical Reference) and the tag.log on the Access Control engine (see 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 Access Control Troubleshooting.

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

Most Severe NAC Events Report



Monitor Access Control Appliance Load

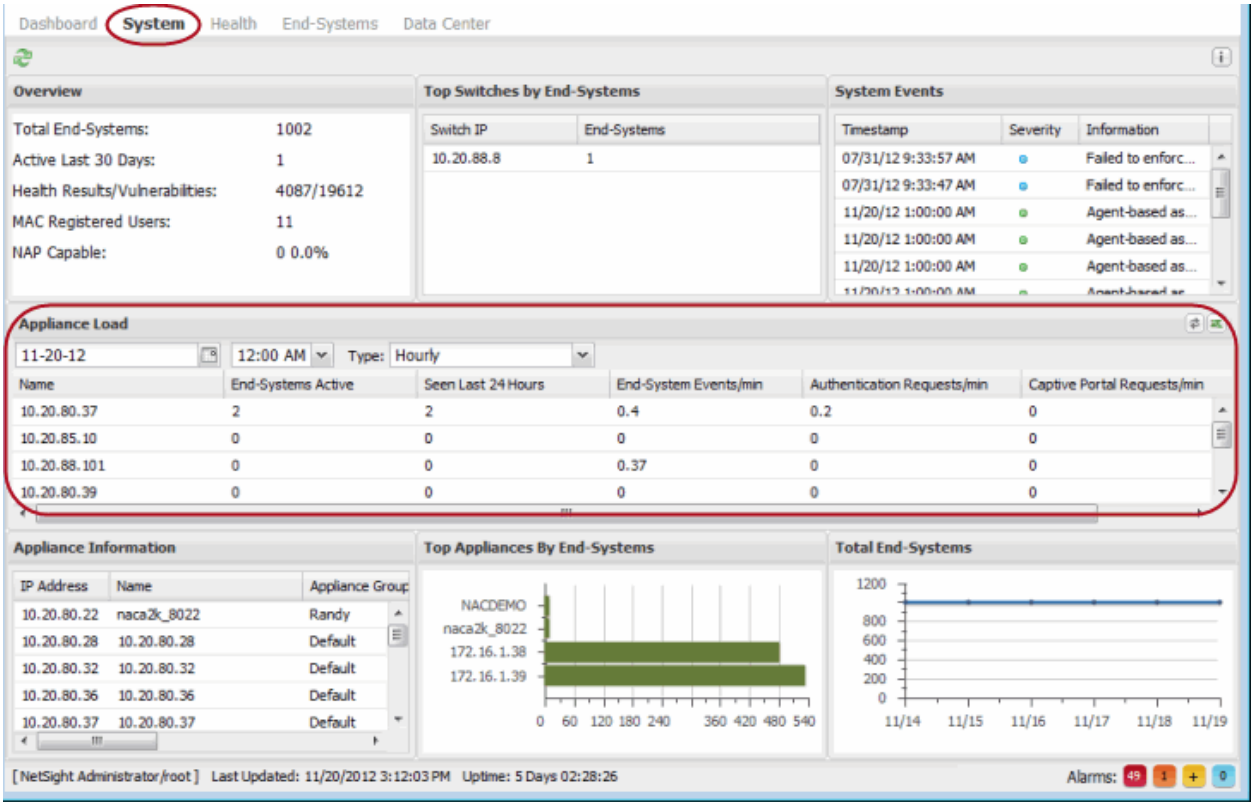
The Access Control Appliance Load report provides a summary of end-system usage for each Access Control engine on the network, including the number of active end-systems on the engine, and the number of authentication and captive portal requests per minute.

This report is useful for determining whether action may be required in order to more evenly distribute the client load among available 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 Access Control hardware.

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

Appliance Load Report



Monitor Access Control End-System Health

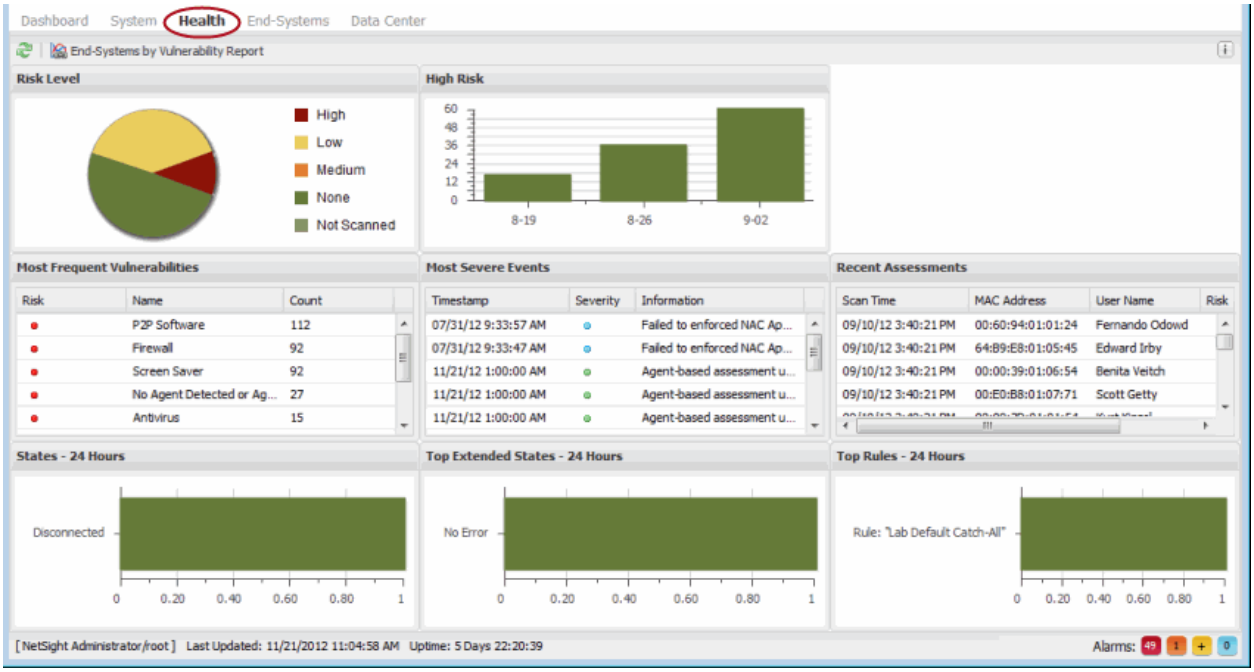
The Access Control Health reports provide information on overall end-system health.

The Risk Level report helps you quickly determine the overall status of threats and vulnerabilities to the entire 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 end-systems 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 Access Control Notifications

Access Control Notifications let you create alerts for when specific events or triggers take place in 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.

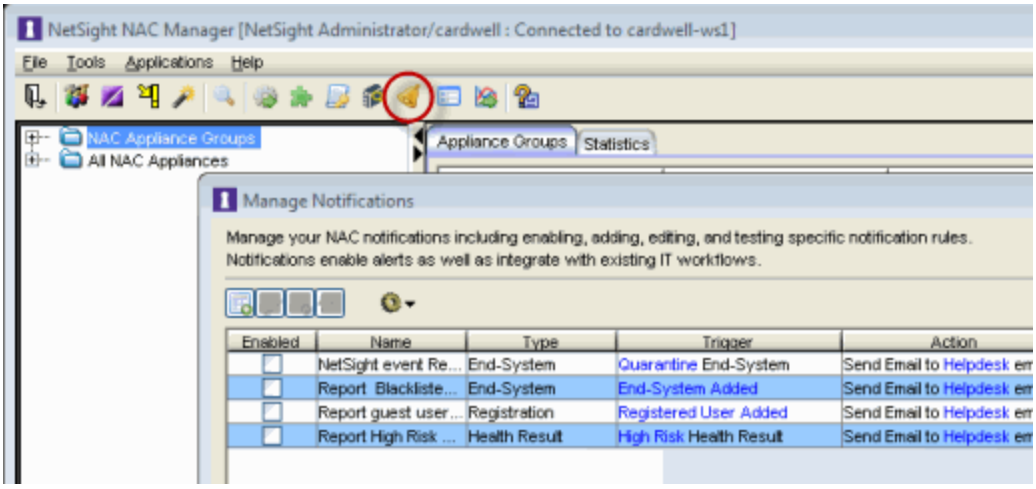
Notifications can be further defined by specific conditions that, in addition to the trigger, determine when actions are performed. For example, you can

configure a condition that filters notifications based on selected engines, user groups, and device groups, as well as 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.

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 Access Control RADIUS Configuration

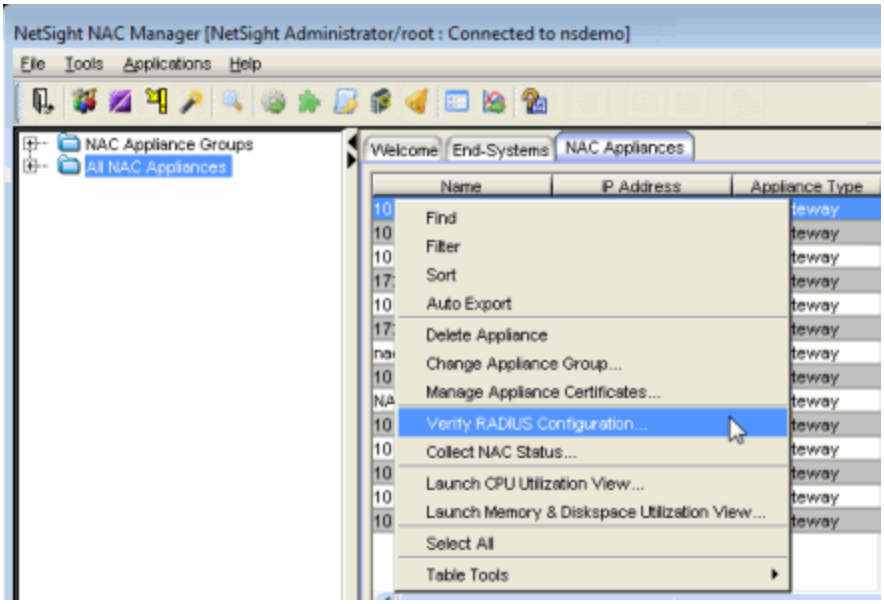
Use the NAC Manager Verify RADIUS Configuration tool to ensure that the RADIUS configurations on your switches are consistent with your Access Control configuration. The verify operation alerts you to any RADIUS configurations that are out of sync and could cause RADIUS authentication problems on the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

Switch RADIUS configurations can be modified independently of 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.

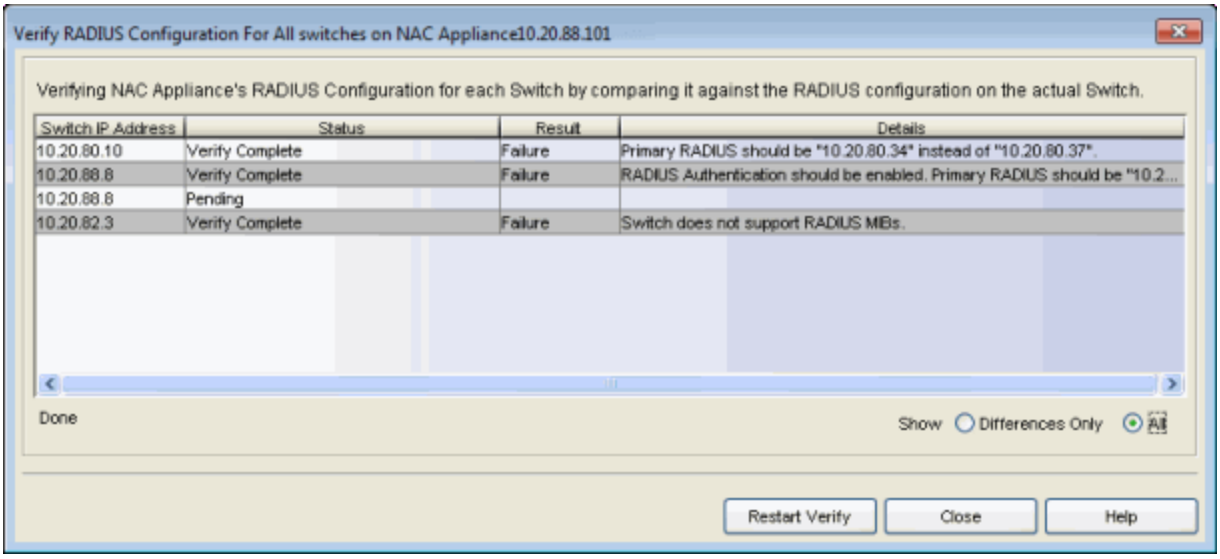
In NAC Manager, right-click on an engine and select Verify RADIUS Configuration as shown here.

Accessing Verify RADIUS Configuration



Verification results are displayed in the Verify RADIUS Configuration window.

Verify RADIUS Configuration Window



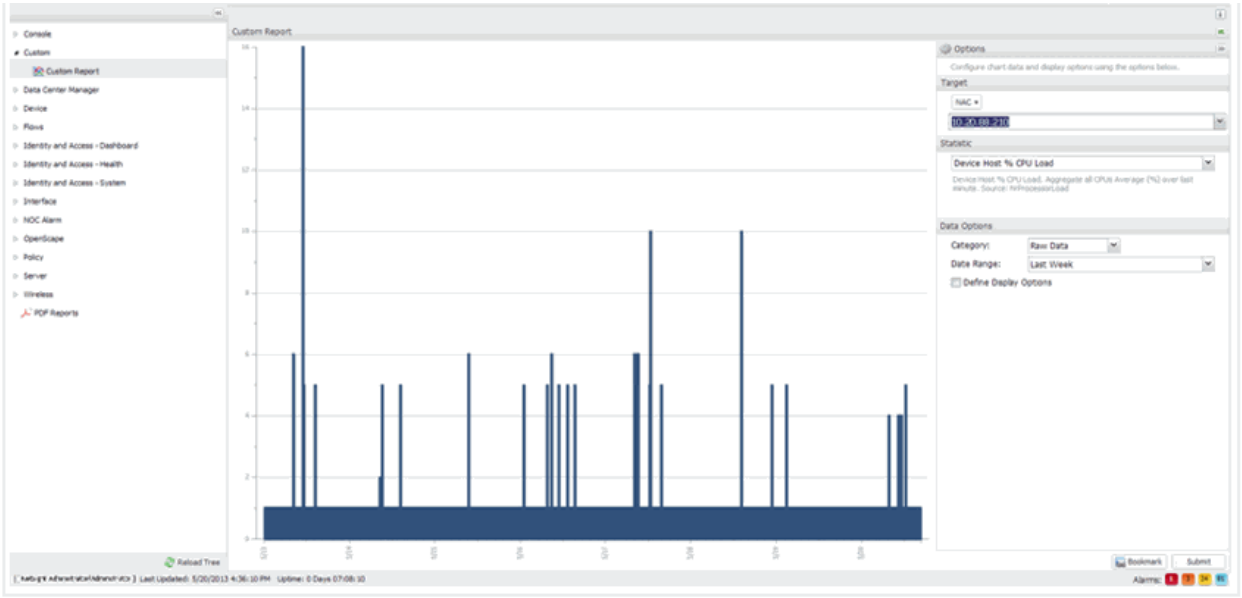
Extreme Management Center Custom Reports

Extreme Management Center Custom Reports let you create specialized reports for monitoring Access Control engine performance. Create reports on a variety of 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 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 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



2/2019
8.2 Revision -00
PN: 9036053-00
Contents Subject to Change Without Notice

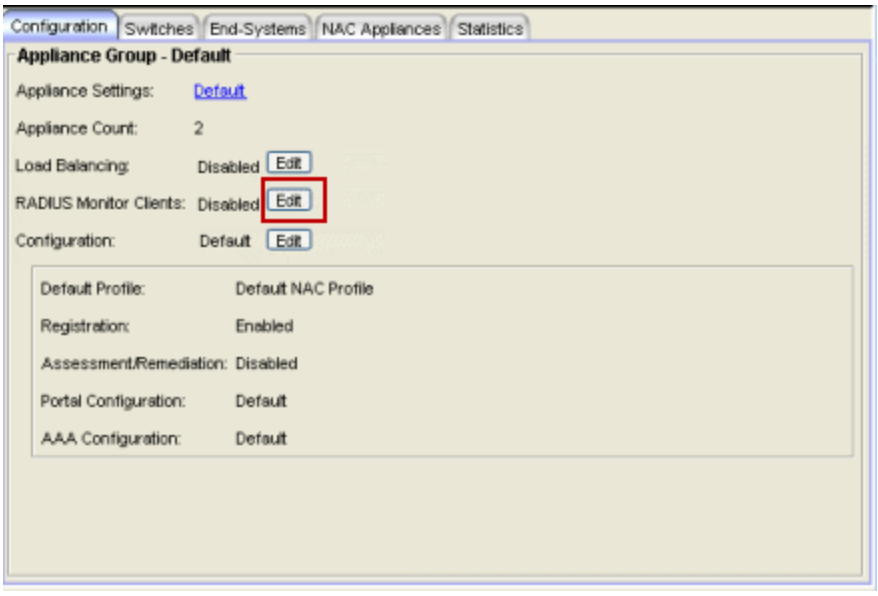
Configure RADIUS Clients to Monitor Access Control Engines in Extreme Management Center (Legacy)

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

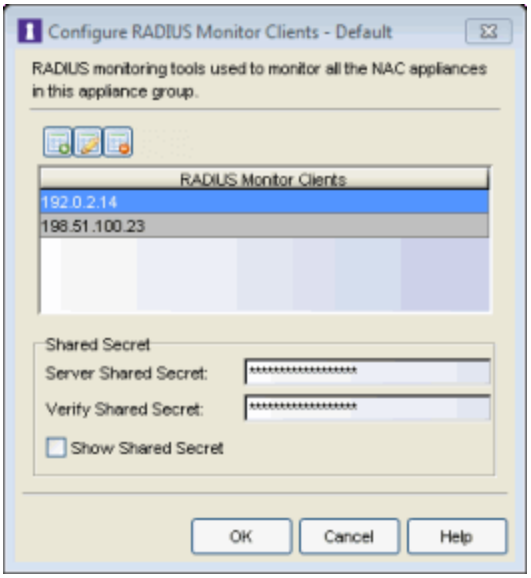
Use the following steps to create a list of RADIUS monitoring clients and configure a special authentication mapping for your AAA configuration used to authenticate the clients.

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.

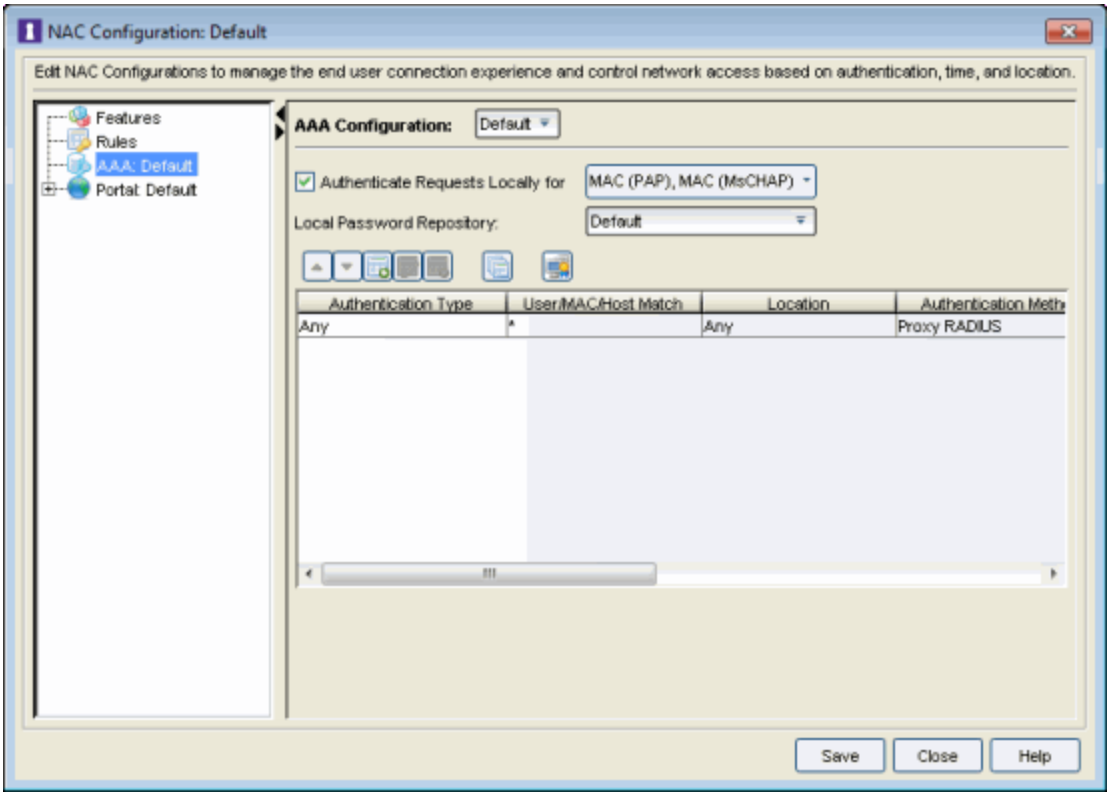


3. The Configure RADIUS Monitor Clients window opens.

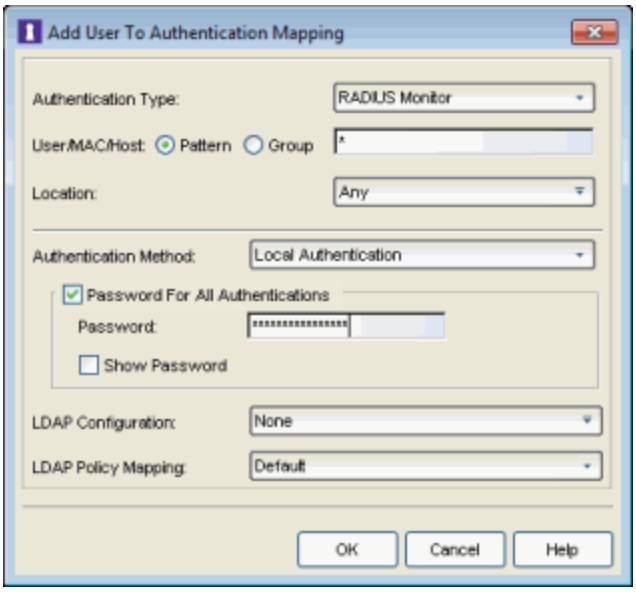


4. Use this window to create a list of the monitoring tools (clients) used, and specify the shared secret to be used for all of them.
    a. Click the button. Enter the IP address for the first client and click **OK**. Repeat for each client that you want to add.
    b. Enter the Server Shared Secret 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.



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.

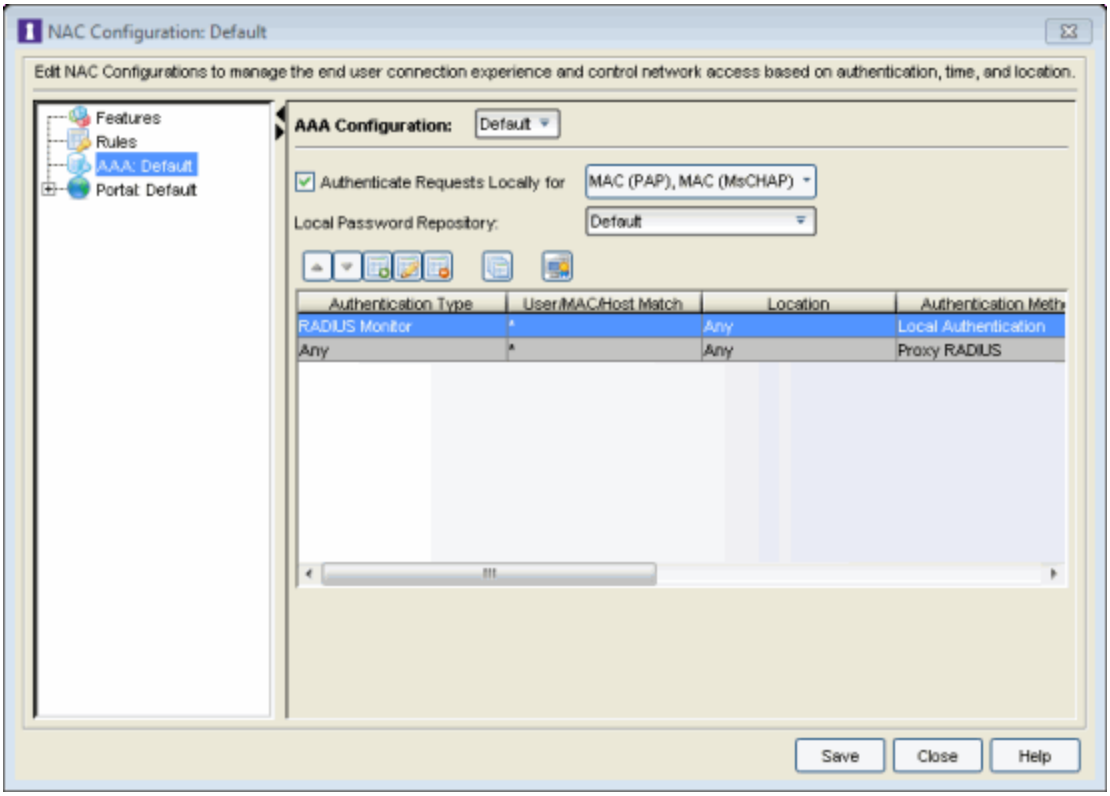


a. Set the Authentication Type to RADIUS Monitor.

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.



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 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

Access Control Performance Tuning in Extreme Management Center

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

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 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 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 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 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

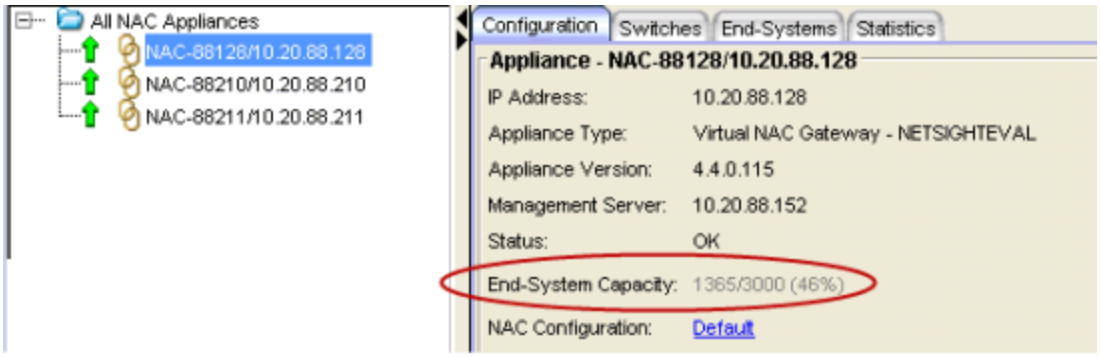
of factors, oversubscribing an engine could lead to scenarios such as failed or intermittent authentication responses, poor end-user experience, or restricted access to the network.

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

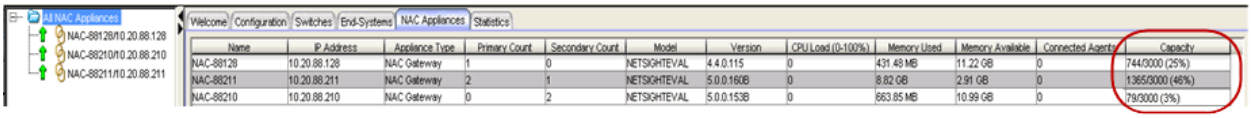
The Configuration tab in NAC Manager displays authenticated end-system and capacity information for each Access Control engine. To view this information, select an Access Control engine in the NAC Manager tree and then select the Configuration tab. The Current Capacity field indicates the number of end-systems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



Engine load reporting is also available within Extreme Management Center. The NAC Appliance Load report provides a summary of end-system usage for each 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.

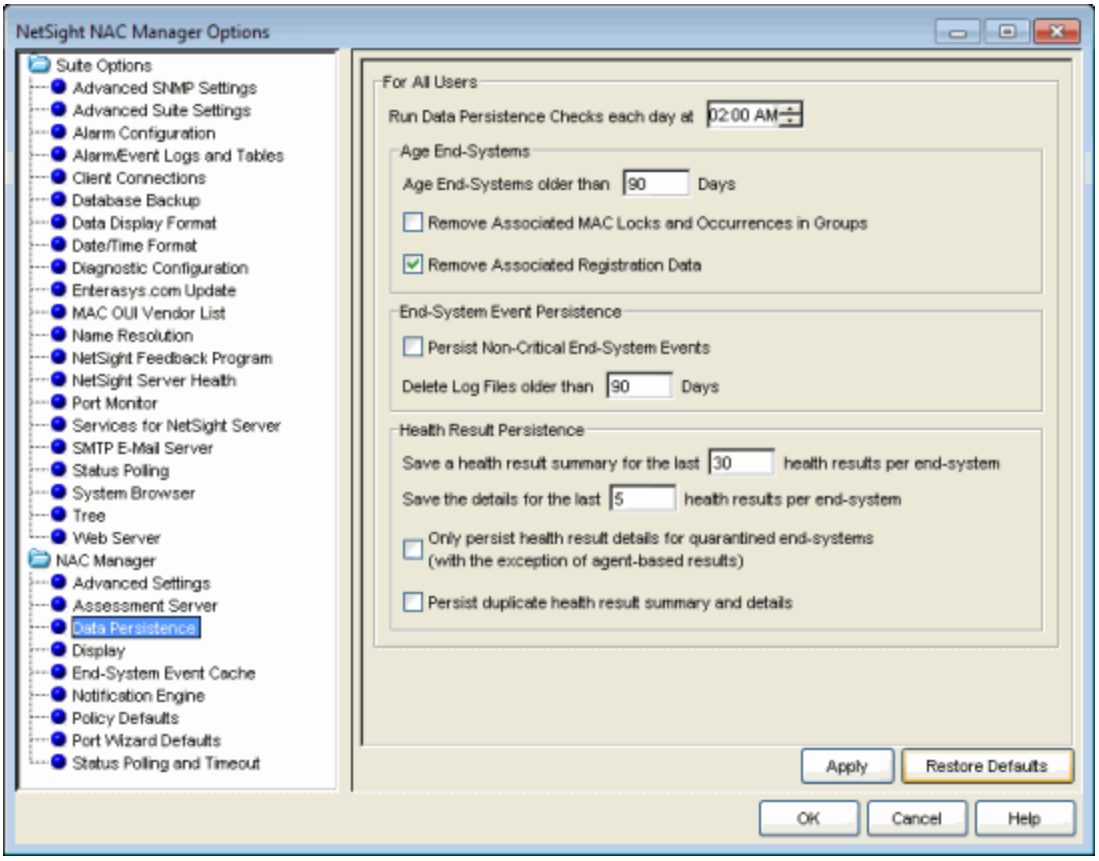
Tuning Data Persistence

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 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 Access Control rule the next time they authenticate to the network, should their end-system 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 end-system and registration information in sync.

End-System Event Persistence

End-system events track authentication and 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 non-critical events include duplicate or unchanging events, such as events tied to re-authentication 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 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 end-system. 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 end-systems, 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 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 Access Control services. These resources are specifically targeted towards the processing of incoming end-systems, end-system events, and health result data sent from Access Control engines to the server. The greater the number of end-systems and engines in your Access Control deployment, the more resources Access Control services require for processing the incoming information updates sent by each Access Control engine.

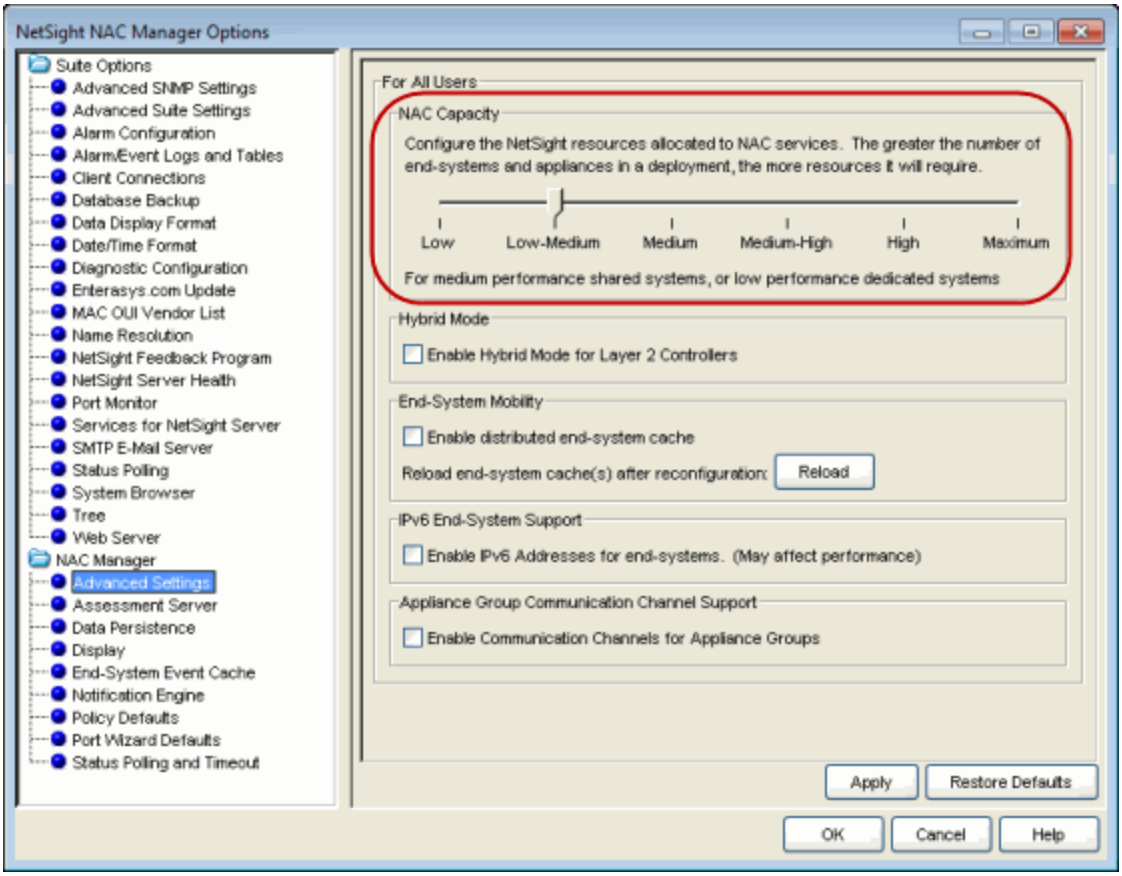
Indications that capacity settings may be insufficient can surface in the form of slower processing of end-system information or possibly missing updates. Modifying the capacity level upwards, incrementally allocates additional server resources dedicated to the processing of this data. Each level provides 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 Access Control deployment.

Insufficient server hardware could appear as an Extreme Management Center performance issue, where in reality, the server hardware resources are not adequate for the deployment. Larger 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 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.

Advanced Settings Options - NAC Capacity



Using 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 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 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 Access Control DNS Proxy to redirect clients to the captive portal.

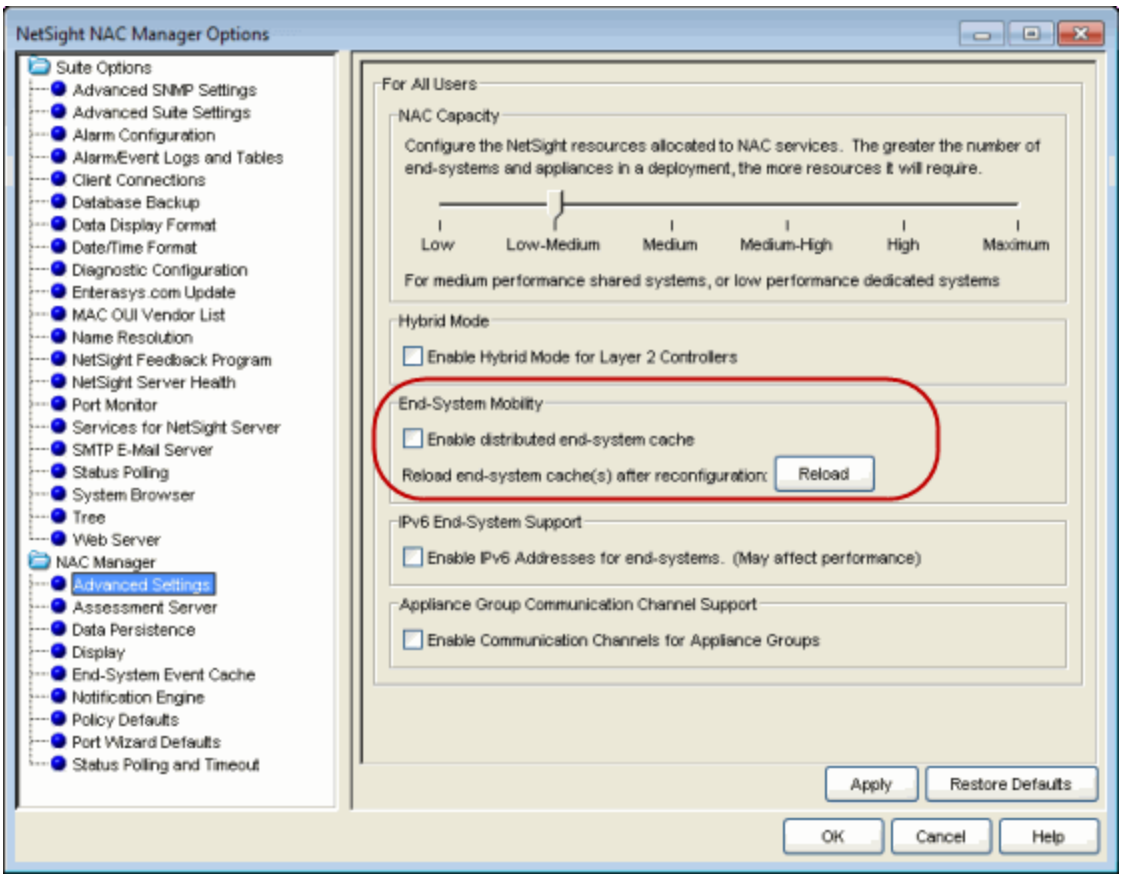
When this feature is enabled, end-system information similar to that in the end-systems table is stored in memory on the Extreme Management Center server and Access Control engine. Each cache contains the same up-to-date information, allowing the engine to perform lookups for end-system information in 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 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 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.

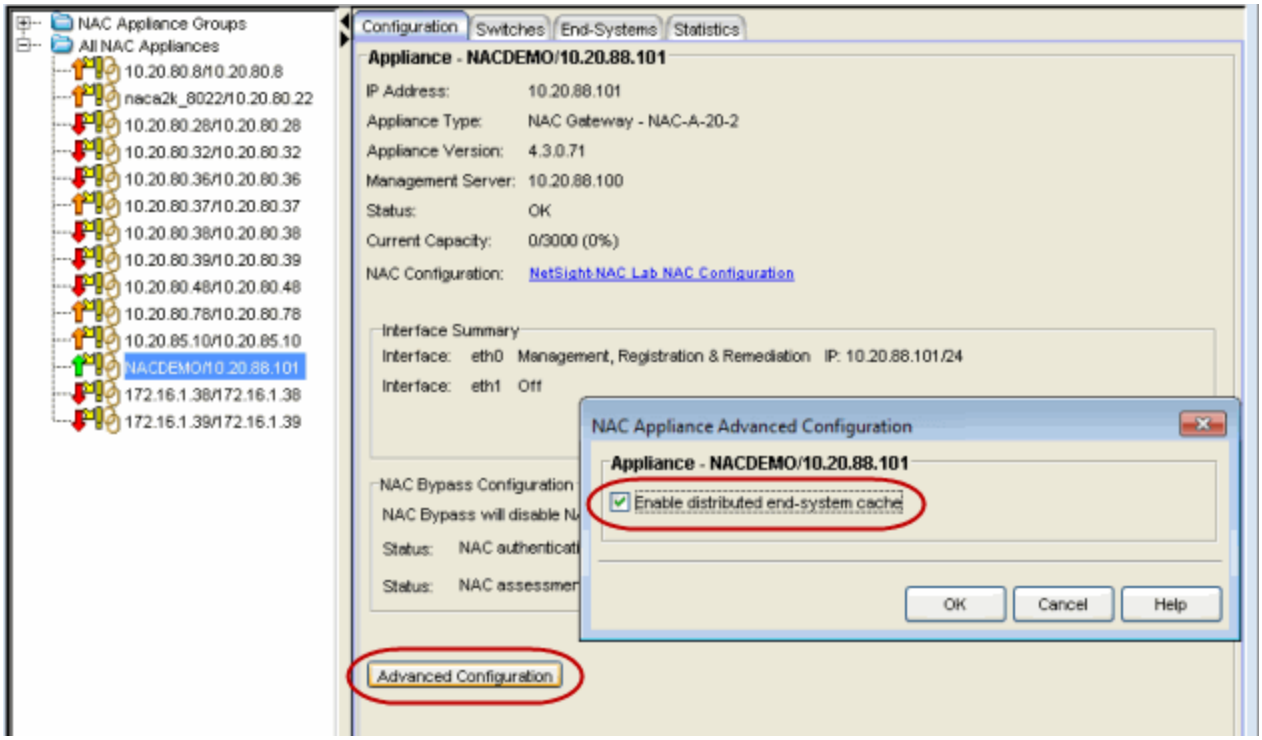
Advanced Settings Options - End-System Mobility



To enable on the 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.

Configuration Tab - Advanced Configuration



NAC Manager and Access Control Troubleshooting in Extreme Management Center

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

- NAC Manager Event Logging
- 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 Access Control engine.

NAC Manager Event View

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 Access Control configuration, and when and for how long communication with an 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 data persistence 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 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 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.

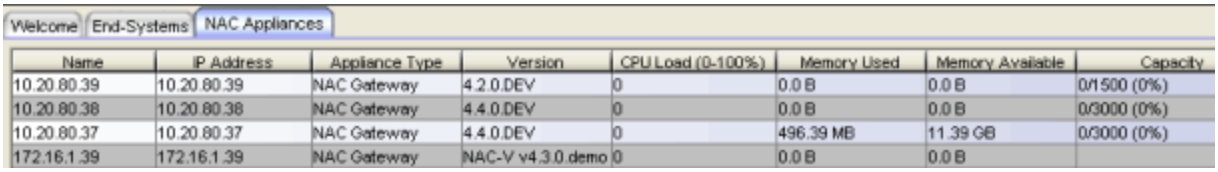
Access Control Engine Real-time Status

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

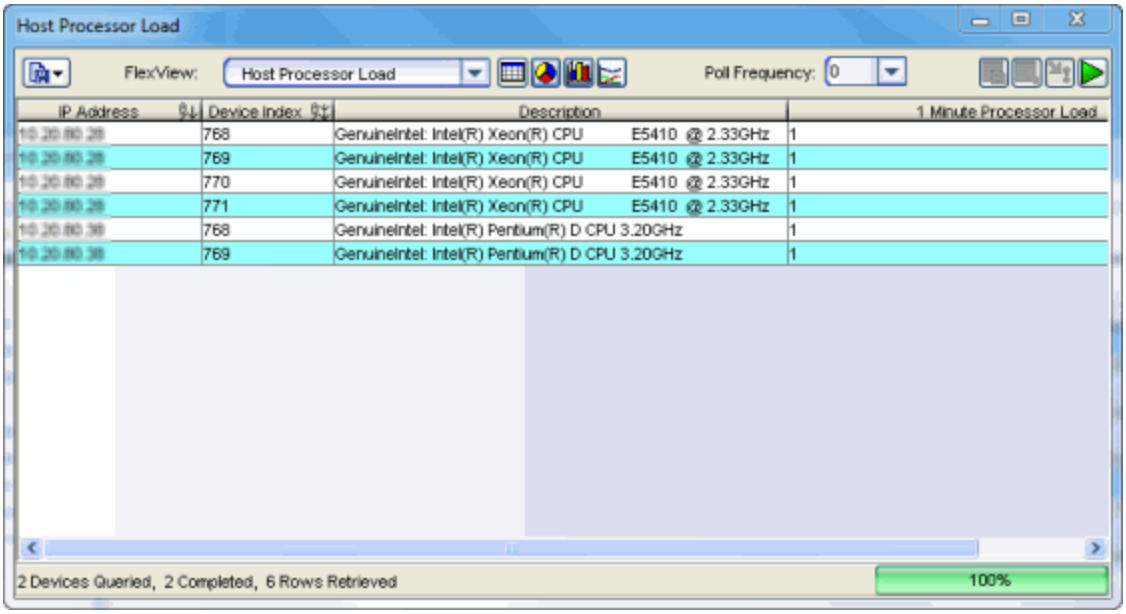
NAC Appliances Tab



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.

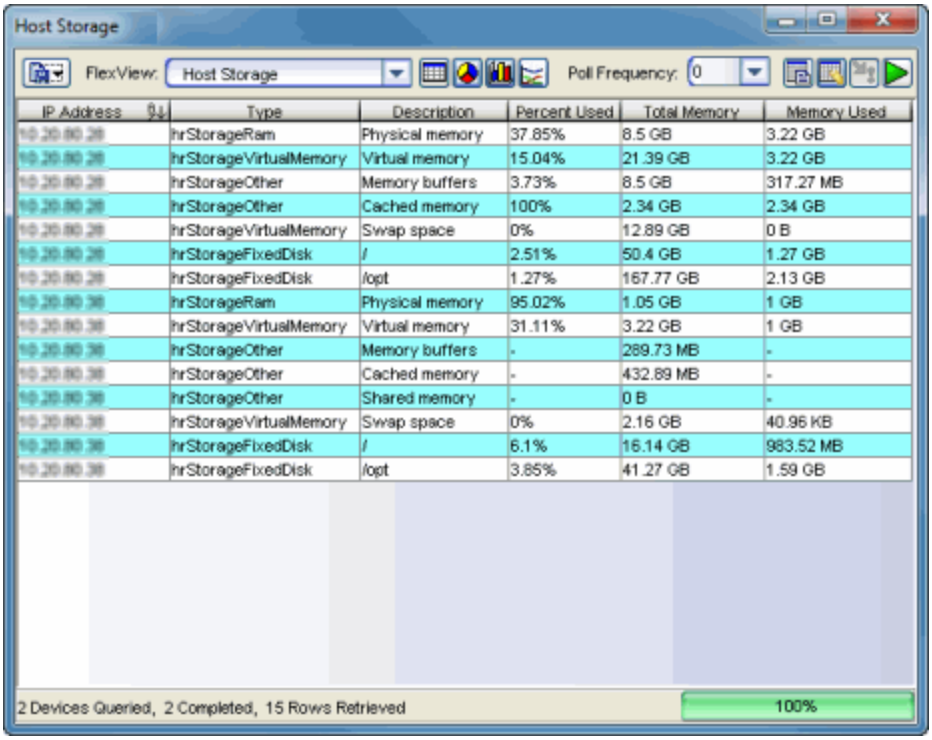
Launch the CPU Utilization View (Host Processor Load FlexView).

Host Processor Load FlexView



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

Host Storage FlexView

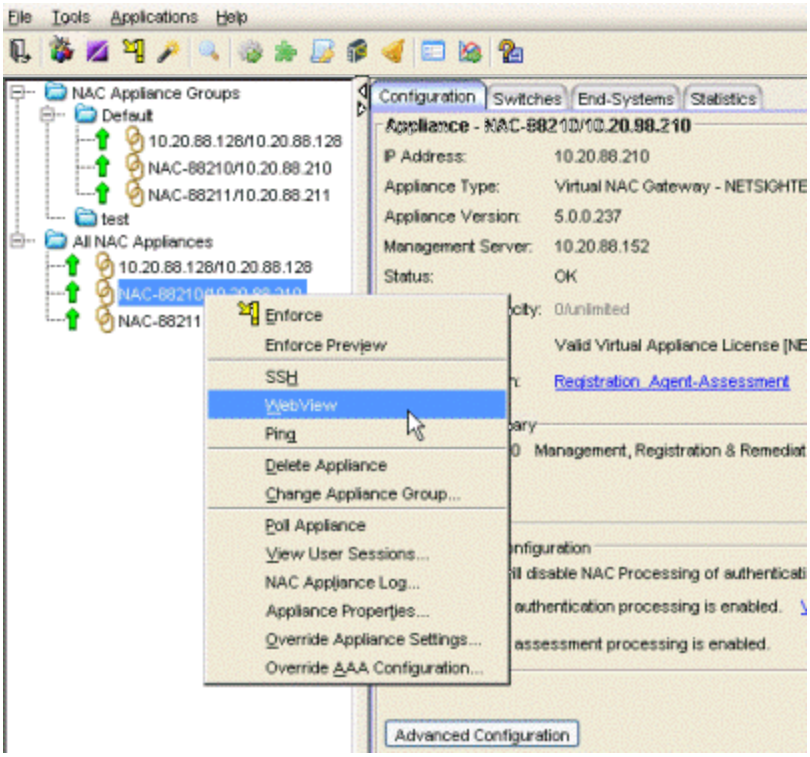


Access ControlEngine Administration Web Page (WebView)

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

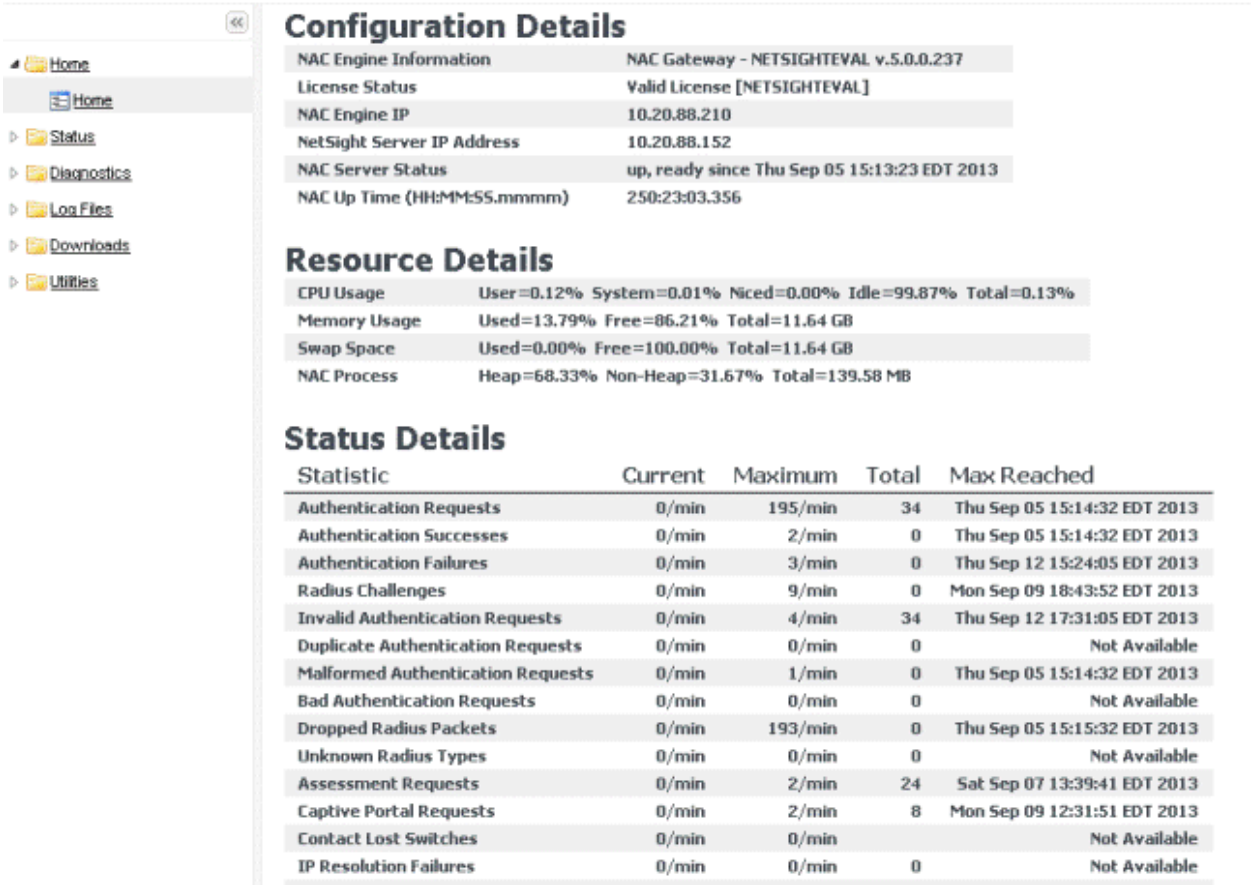
Launch WebView



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



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

Access Control Switches and Routers

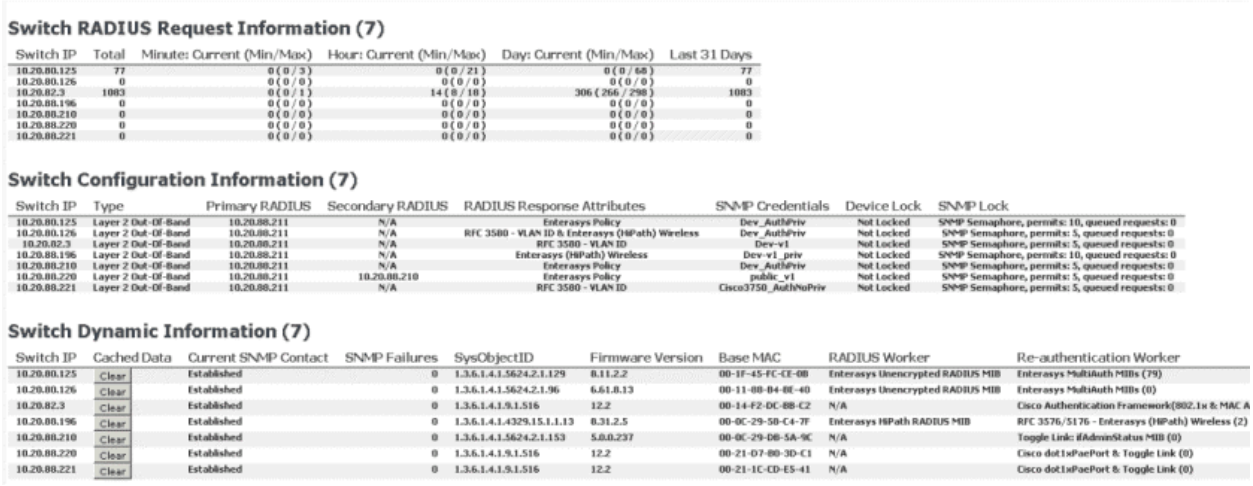
When troubleshooting issues involving authentication, IP resolution, and re-authentication (etc.), the Switches & Routers page within WebView provides a variety of useful real-time data.

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.

The Switch Configuration section is an overview of all switches assigned to the Access Control engine, the RADIUS response attributes they are configured for, and the SNMP credential the Access Control engine is using to communicate with the switch. This information can be used to identify whether the 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 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 Access Control engine to the switch, which may be different than from Extreme Management Center Console to the switch.

Engine Administration Web Page



Switch RADIUS Request Information (7)

Switch IP	Total	Minute: Current (Min/Max)	Hour: Current (Min/Max)	Day: Current (Min/Max)	Last 31 Days
10.20.80.125	77	0 (0 / 3)	0 (0 / 21)	0 (0 / 68)	77
10.20.80.126	0	0 (0 / 0)	0 (0 / 0)	0 (0 / 0)	0
10.20.82.3	1083	0 (0 / 1)	14 (8 / 10)	306 (266 / 298)	1083
10.20.88.196	0	0 (0 / 0)	0 (0 / 0)	0 (0 / 0)	0
10.20.88.210	0	0 (0 / 0)	0 (0 / 0)	0 (0 / 0)	0
10.20.88.220	0	0 (0 / 0)	0 (0 / 0)	0 (0 / 0)	0
10.20.88.221	0	0 (0 / 0)	0 (0 / 0)	0 (0 / 0)	0

Switch Configuration Information (7)

Switch IP	Type	Primary RADIUS	Secondary RADIUS	RADIUS Response Attributes	SNMP Credentials	Device Lock	SNMP Lock
10.20.80.125	Layer 2 Out-Of-Band	10.20.88.211	N/A	Enterasys Policy	Dev_AuthPriv	Not Locked	SNMP Semaphore, permits: 10, queued requests: 0
10.20.80.126	Layer 2 Out-Of-Band	10.20.88.211	N/A	RFC 3580 - VLAN ID & Enterasys (HiPath) Wireless	Dev_AuthPriv	Not Locked	SNMP Semaphore, permits: 5, queued requests: 0
10.20.82.3	Layer 2 Out-Of-Band	10.20.88.211	N/A	RFC 3580 - VLAN ID	Dev-v1	Not Locked	SNMP Semaphore, permits: 5, queued requests: 0
10.20.88.196	Layer 2 Out-Of-Band	10.20.88.211	N/A	Enterasys (HiPath) Wireless	Dev-v1_priv	Not Locked	SNMP Semaphore, permits: 10, queued requests: 0
10.20.88.210	Layer 2 Out-Of-Band	10.20.88.211	N/A	Enterasys Policy	Dev_AuthPriv	Not Locked	SNMP Semaphore, permits: 5, queued requests: 0
10.20.88.220	Layer 2 Out-Of-Band	10.20.88.211	10.20.88.210	Enterasys Policy	public_v1	Not Locked	SNMP Semaphore, permits: 5, queued requests: 0
10.20.88.221	Layer 2 Out-Of-Band	10.20.88.211	N/A	RFC 3580 - VLAN ID	Cisco3750_AuthNoPriv	Not Locked	SNMP Semaphore, permits: 5, queued requests: 0

Switch Dynamic Information (7)

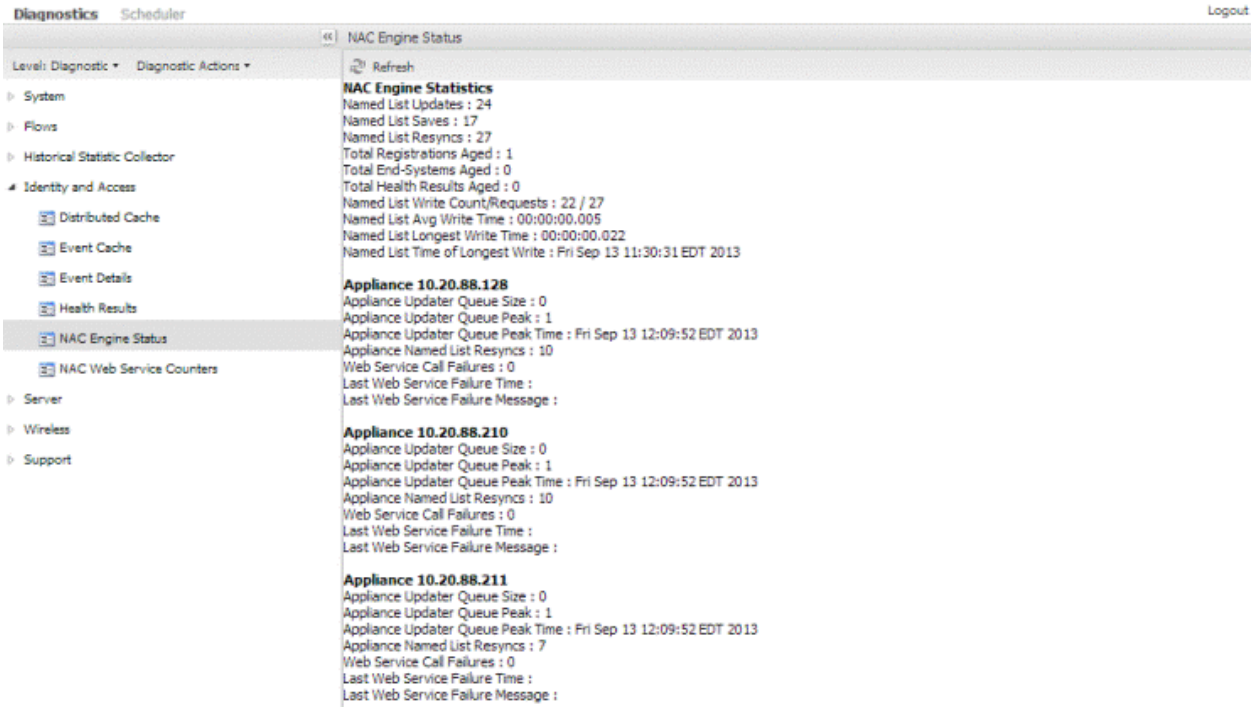
Switch IP	Cached Data	Current SNMP Contact	SNMP Failures	SysObjectID	Firmware Version	Base MAC	RADIUS Worker	Re-authentication Worker
10.20.80.125	Clear	Established	0	1.3.6.1.4.1.5624.2.1.129	8.11.2.2	00-1F-45-FC-CE-08	Enterasys Unencrypted RADIUS MIB	Enterasys MultiAuth MIBs (79)
10.20.80.126	Clear	Established	0	1.3.6.1.4.1.5624.2.1.96	6.61.8.13	00-11-88-B4-8E-40	Enterasys Unencrypted RADIUS MIB	Enterasys MultiAuth MIBs (0)
10.20.82.3	Clear	Established	0	1.3.6.1.4.1.9.1.516	12.2	00-14-F2-DC-88-C2	N/A	Cisco Authentication Framework(802.1x & MAC A
10.20.88.196	Clear	Established	0	1.3.6.1.4.1.4329.15.1.1.13	8.31.2.5	00-0C-29-50-C4-7F	Enterasys HiPath RADIUS MIB	RFC 3576/5176 - Enterasys (HiPath) Wireless (2)
10.20.88.210	Clear	Established	0	1.3.6.1.4.1.5624.2.1.153	5.0.0.237	00-0C-29-D8-5A-9C	N/A	Toggle Link: ifAdminStatus MIB (0)
10.20.88.220	Clear	Established	0	1.3.6.1.4.1.9.1.516	12.2	00-21-D7-80-3D-C1	N/A	Cisco dot1xPaePort & Toggle Link (0)
10.20.88.221	Clear	Established	0	1.3.6.1.4.1.9.1.516	12.2	00-21-1C-CD-E5-41	N/A	Cisco dot1xPaePort & Toggle Link (0)

Extreme Management Center Administration - Identity and Access

The Administration tab in Extreme Management Center has an Identity and Access section that provides detailed diagnostic and statistical information pertaining to advanced 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



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 Access Control engine CLI and can be executed to provide detailed data regarding the 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 Access Control engines.

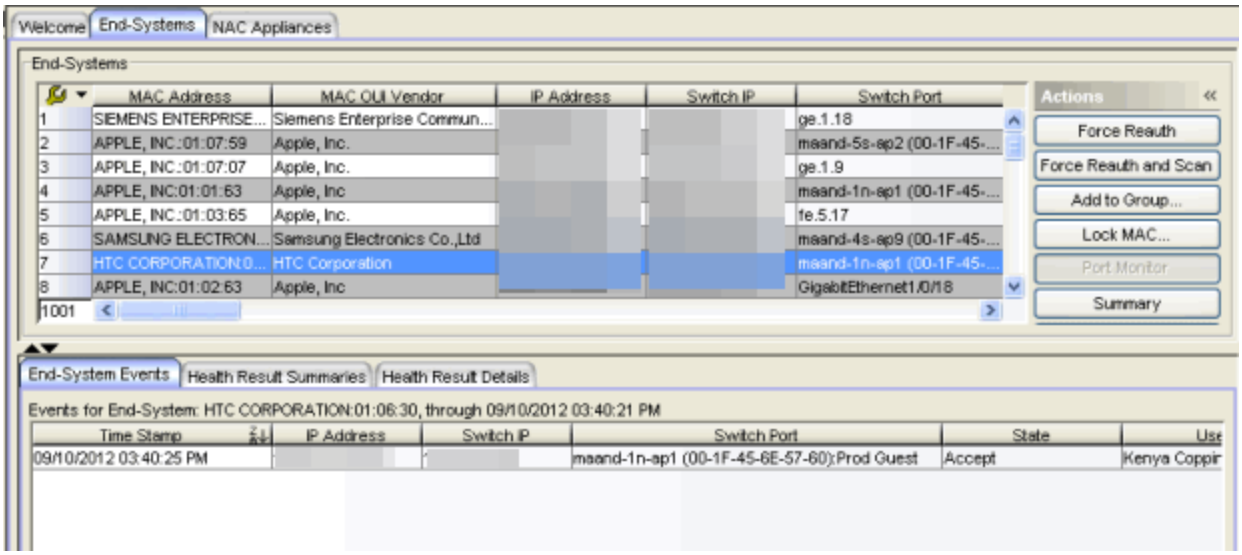
End-System Troubleshooting

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

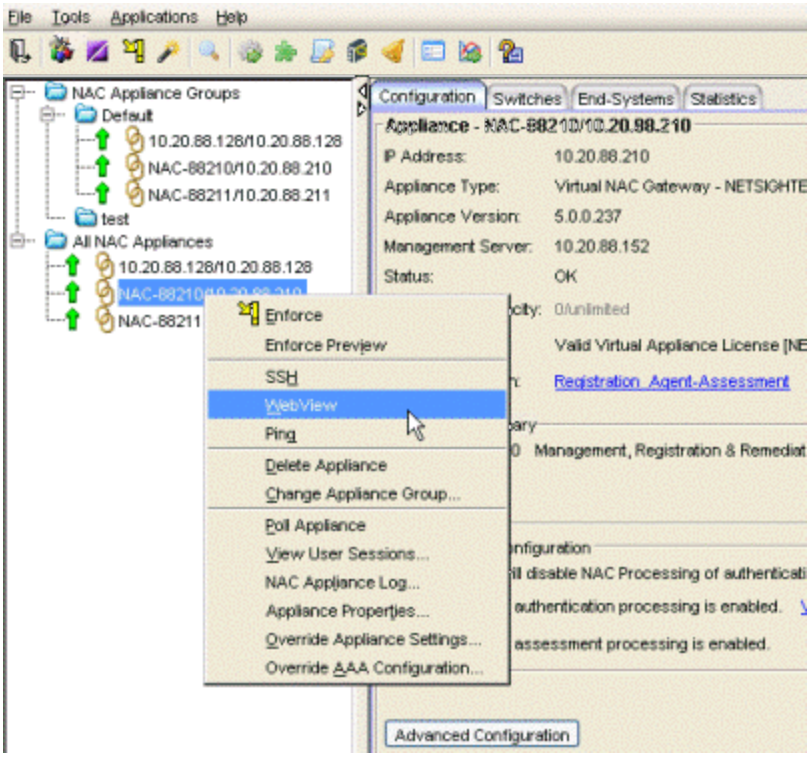


Engine End-System Diagnostics

To access end-system diagnostic information for a specific Access Control engine, launch the Access Control engine administration web page by right-clicking on an 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://<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.

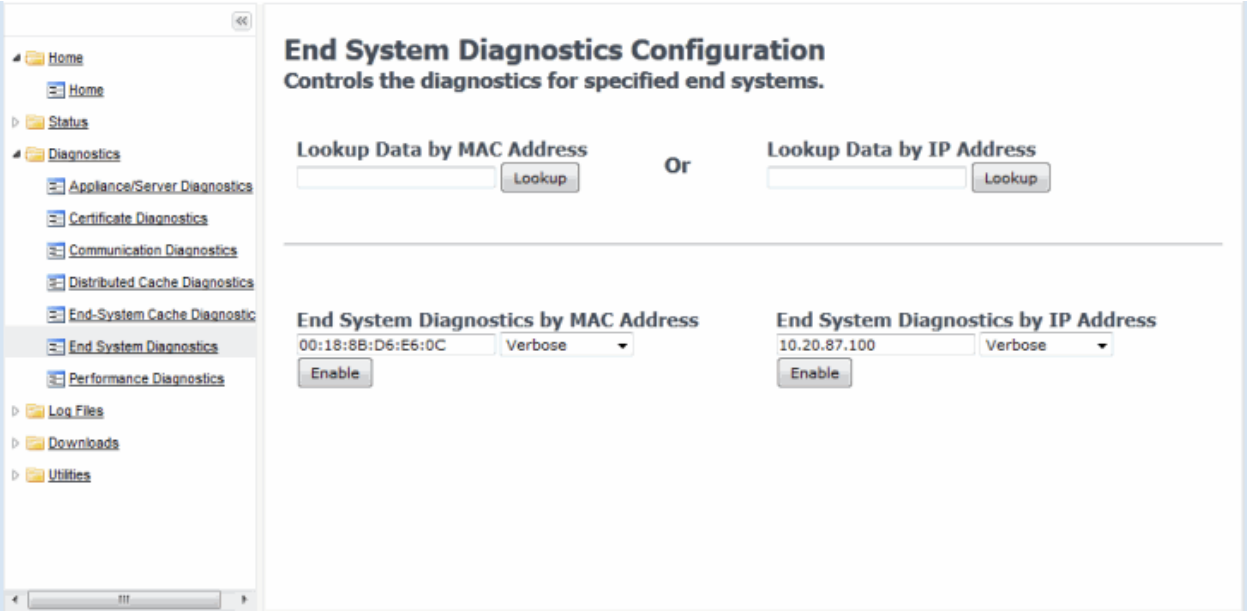
Targeting diagnostics for a specific end-system enables a majority of the debug diagnostics available on a global level, but only for the specific end-system. Therefore, diagnostics can be enabled for an extended period of time without the concern of generating the excessive log files that are possible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

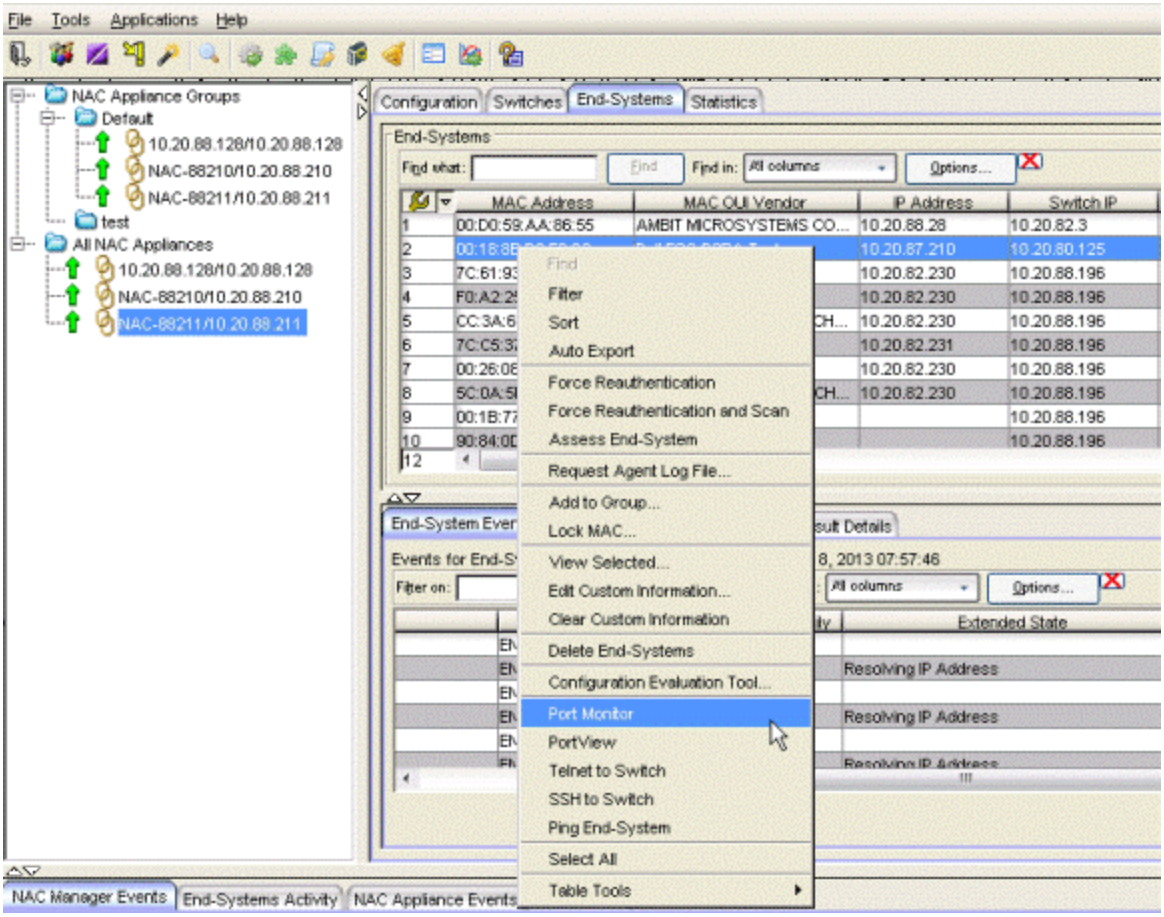
Engine End-System Diagnostics



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



- 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 Access Control engine.
- Port Monitor - View detailed port and switch status information for the selected end-system 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 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.

2/2019
8.2 Revision -00
Contents Subject to Change Without Notice