Central Manager Overview
How-to Guide
Central Manager is a two-tier (client/server) system that allows you to manage multiple IVEs, regardless of whether or not they are clustered. The Central Manager includes:

- **System dashboard**—displays system capacity graphs and alarms that allow you to easily monitor the system. You can access the system dashboard from the **System > Status** page of the Web console.

- **Improved logging and monitoring**—allows you to create custom filters so that you may view and save only those log messages that you choose in the format of your choice. You can access the logging feature from the **System > Log/Monitoring** page of the Web console.

- **Push configuration feature**—allows you to easily push settings from one IVE to another for convenient centralized management. You can access the push configuration feature from the **Maintenance > Push Config** page of the Web console.

- **Zero downtime upgrades**—allows you to expedite upgrades across a cluster, ensuring that one cluster member is always functional during the upgrade process. You can access the upgrade feature from the **Maintenance > System > Upgrade/Downgrade** page of the Web console.

- **Improved user interface**—The Web console for Central Manager includes an enhanced appearance over the standard Web console for appliances with a baseline license.

### Upgrading/Creating clustered nodes

The Pulse Secure NetScreen-SA Central Manager offers the ability to easily upgrade every node in a cluster. You simply install a newer service package on one node and, once the installation completes and the node reboots, the node pushes the service package to all nodes in the cluster.

If you have not purchased the Pulse Secure NetScreen-SA Central Manager you can still upgrade clustered nodes, but the process requires you to disable nodes within the cluster, upgrade them individually, and then enable them within the cluster again.

For more information about disabling nodes to upgrade the service package, see “Upgrade the cluster service package” in the administration guide.

If you purchased the Pulse Secure NetScreen-SA Central Manager, you can create a cluster using the IVE running the latest OS version and then add additional nodes using the “upgrade and join” functionality. When you add a node to a cluster using this feature, the first IVE node upgrades the joining node with the more current service package. This functionality works only when all the IVEs are running version 4.0 or later of the OS.

For more information see “Clustering overview” in the administration guide.

### Custom filter log files

The Central Manager package allows you to filter and format the data in your events, user access, and administrator access log files. When you filter log files, the IVE appliance only saves those messages specified within the filter query. For example, you may create a query that only logs entries for a particular range of IP addresses or for users who are signed into a specific realm. To create a query, use the IVE custom expression language.
When you format log files, the IVE appliance simply changes the “look” of the log messages based on your specifications. Log formats do not affect which data the appliance saves; formats only affect how the appliance displays the data. An IVE appliance includes standard, WELF, and W3C log formats, but you may also choose to create your own custom format. To create a custom format, use log fields.

For configuration instructions, see “Configuring the Log Monitoring page” in the administration guide.

Dynamic log filters

The Central Manager package provides administrators with the ability to quickly change the log view by clicking on any data log variable link in the currently viewed log. For instance, if you want to temporarily view the User Access Log based on a particular IP address, create a “quick filter” by clicking on any occurrence of that IP address in the current log and the IVE immediately redraws the log to show all entries containing the specified IP address. Furthermore, clicking on additional data log variable links expands the quick filter and updates the current view of the log.

Although quick filters act as temporary filter agents, the IVE gives you the option of saving the temporary query strings a new custom filters.
For configuration instructions, see “Create, reset, or save a dynamic log query” in the administration guide.

Creating local backups of IVE configuration files

IVE appliances equipped with the Central Manager license enable you to save backups of your current system configuration and user accounts directly to the IVE in binary format. You may then use these configurations to restore the IVE or a cluster of IVEs to the state contained in the encrypted file. Note that these files only contain configuration information—they do not include logs.

You may save up to 5 system configuration backups and 5 user account backups on the IVE. If you try to exceed this limit, the IVE overwrites the oldest backup with the new backup. If you do not want to overwrite the oldest backup, choose another backup to delete instead, before saving the most current one.

You may use system and user backups to update a single IVE or a cluster. If you choose to restore an IVE that is enabled as part of a cluster, that IVE automatically pushes the configuration to all other cluster members. The cluster is disabled until all cluster members have updated their settings using the backup configuration. Then, they restart and re-enable the cluster.

You can create backups from the Maintenance > Archiving > Local Backups page of the Web console.

For instructions, see “Local Backups tab” in the administration guide.
Pushing configurations from one IVE to another

IVE appliances enabled with the Central Manager license enable you to copy selected configuration settings from one IVE to another using the Push Configuration feature. This feature provides simple configuration management across an enterprise without requiring you to cluster IVE appliances. With the Push Configuration feature, you can decide exactly which settings you do and do not want to copy across the enterprise. The Push Configuration feature uses the same functionality as that provided by the XML Import/Export feature to create XML instance files, which the Push Configuration feature then pushes to another IVE.

For instructions, see “Configuring the Push Config page” in the administration guide.

Prior to using Push Config, you must configure your system following specific conditions:

- You must map to the Administrators role, thereby creating a “super administrator” with full administration privileges.
- The target IVE administrator account must use static password authentication or two-factor tokens that do not use challenge-response type authentication. For example, certificates, Soft ID, and Defender Authentication are not supported.
- You must not configure the administrator account in a way that requires the administrator to select a role to sign in to the target IVE. For example, you must not map a single user to multiple roles, including the push configuration administrator role, and then fail to permissively merge those roles. We recommend creating an account exclusively for push configuration administrators to guarantee that the administrator does not need to choose a role during the sign-in process and to clearly distinguish the actions of push configuration administrators in your log files.
View system capacity utilization

The Central Manager dashboard for Access Series and Meeting Series appliances provides system capacity utilization graphs that allow you to easily view and understand how much of your system capacity you are using on a regular basis. To use this information for data reporting elsewhere, export it as an XML file using options on the Maintenance > Import/Export > Configuration page.

These graphs are displayed in the System > Status > Overview tab when you open the Web console, and allow you to easily view:

- **Concurrent Users**—this graph shows the number of users signed into the IVE. In clustered environments, the graph includes two lines. The first line displays the number of local users signed into the node selected from the drop-down list and the second line displays the number concurrent users signed into the entire cluster.

- **Concurrent Meetings (Secure Meeting appliance only)**—this graph shows the number of meetings that are currently in progress. In clustered environments, the graph includes two lines. The first line displays the number of meetings running on the node selected from the drop-down list and the second line displays the number meetings running on the entire cluster.

- **Hits Per Second**—this graph shows the number of hits currently being processed by the IVE. In a clustered environment, you may choose an IVE from the drop-down list to determine which node’s data is displayed in the graph. The graph includes four lines: number of hits, number of Web hits, number of file hits, and number of client/server hits.
• **CPU and Virtual (Swap) Memory Utilization**—this graph shows the percentage of the CPU and available memory currently being used. In a clustered environment, you may choose an IVE from the drop-down list to determine which node's data is displayed in the graph.

• **Throughput**—this graph shows the amount of data (in KB) currently being processed. In a clustered environment, you may choose an IVE from the dropdown list to determine which node's data is displayed in the graph. The graph includes four lines: external in, external out, internal in, and internal out. You may also use the Page Settings window to configure which graphs the IVE displays in the dashboard and the period of time that the IVE tracks.

View critical system events

The Central Manager dashboard for Access Series and Meeting Series appliances allows you to easily view the last 10 critical system events. Using the Event Monitor window, you can quickly access and address any critical system problems. Once you have opened the Event Monitor window, you may keep it open and continually monitor system events while navigating through the Web console to perform standard maintenance and configuration tasks.
To quickly review critical system events:

1. In the Web console, choose **System > Status > Overview**.

2. Click **Critical Events**. The **Event Monitor** window displays the severity and message of any critical events recorded in the system’s log file.

3. Click **Refresh** to view the most up-to-date events (optional).

4. Click **See All** to navigate to the **System > Log/Monitoring > Events > Log** tab, where all events—ranging from informational to critical—are displayed (optional).

For more information, see “Configuring the Log Monitoring page” in the administration guide.

---

### System Status

**Critical Events**

**System Version**

5.0.1 (build 8555)

**Download Package**

**Last Reboot**

21 days, 1 hour, 23 minutes, 26 seconds

**System Date & Time**

2005-07-13 07:48:13 AM

**Logging Disk**:

0% Full

**Max Licensed Users**: 2500

**Signed-In Users**: 1

**Signed-In Mail Users**: 0

---

**Download the current service package**

The **System > Status > Overview** tab allows you to download the service package that is currently installed on the IVE so that you may easily save it and install it on another IVE.
To download your current service package:

1. In the Web console, choose System > Status > Overview.

2. Click Download Package (Central Manager Versions) or the link next to System Software Pkg Version.

3. Click Save.

4. Specify a name and location for the service package.

5. Click Save.

Central Manager Dashboard Graphs XML

For details see Appendix F in administration guide.