CHAPTER 8

Creating audits and reports

This chapter tells you how to create audits and reports.

OverDrive provides state-of-the art reporting for application access and network security.

Rationale for reports

Not only do you as an admin need reports and logs to manage a network to assure that it's working properly, that you can track down errors flagged against devices and business properties, and so on, but you must repair specific reports as required by federal regulations.

Generating an audit log

Audit logs record detailed information such as which:

- Admins have logged in, when, and in which roles
- Objects have been created, edited, renamed, or deleted
- Permissions have been granted, edited, or removed
- Resources have been resigned to which policies
- Policies that have been implemented, edited, or deleted

To generate an audit log:

1. Click the Launch Audit Log icon in the icon toolbar.
2. Choose one of the following:
   - Click Load to load the current file
   - Or specify a different file, and/or a date range, and/or a search string (check As Regular Expression if needed), as appropriate, and then click Load.

3. Search for the appropriate information, or copy the window contents to paste into a file for further analysis.

Generating HIPAA, PCI, and SOX reports

OverDrive delivers secure VPN access, network access policies, and access control rules for defined users or groups of users, ensuring that only business-policy specified users may access the applications defined by one or more business policies. This type of access security can be shown to comply with federal regulations.

OverDrive provides a mechanism for reporting back all of the rules and configurations that have been derived from business policies. This is an invaluable tool for building reports for HIPAA (Health Insurance Portability and Accountability Act) PCI (Payment Card Industry), and SOX (Sarbanes Oxley) regulations.

The reports show the defined policies, all users or groups of users associated with the policies, the applications and data sources associated with the policies, and the actual configuration statements in the devices that support the policies.

To generate such reports:

1. In the network status view, do one of the following:
   - Right-click on a site to generate a report of the connections in place at that site (see below).
   - Click on a domain to generate a report for all sites in that domain.

Creating site compliance reports

To generate a site compliance report from the network hardware status view:

1. Display the network status view.
2. Highlight a particular site or domain.
3. Generate the compliance report by choosing from the following:
   - For a site, choose Export Site Compliance Report.
   - For a domain, choose Export Combined Sites Compliance Report.

4. Browse to the directory you want, then click Export.

   The report is saved as a text file.

For examples, see the "Site and domain compliance reports" section on page B-1