globalvelocity
Next generation cybersecurity solutions

# GV-2010 Product Overview Guide

Through real-time inspection and re-assembly of all TCP traffic, the GV-2010 provides packet level visibility into the data moving across networks providing unprecedented ability to identify threats, classify information and control applications. Listed below is a sampling of prized digital assets the GV-2010 can protect:

- **Financials**
  - Credit card numbers for Payment Card Industry (PCI) compliance
  - Institution financials
  - Staff, student and/or parent information
  - Donors' private contact information and contribution history
- **Personally Identifiable Information (PII)** for staff, contractors, students and/or parents
  - Social security numbers
  - Address, telephone number, e-mail, DOB, etc.
  - Student academic records
- **Research & Development**
  - Intellectual property and patents
  - Research involving export control
- **Human Resources**
  - Staff salaries
  - Confidential contracts and agreements
  - Performance reviews
- **Medical Records & Research**
  - Clinical studies analysis and results
  - Identification of ICD codes and/or other medically related codes
  - Health Information Portability and Accessibility Act (HIPAA) compliance

## Content Visibility

The GV-2010 offers four data inspection techniques to protect confidential information:

- **Unstructured Data** - Provides protection of documents and their contents. The GV-2010 “fingerprints” specific documents or the contents of a network repository and flags the movement of its information regardless of whether its format has been changed (such as Word to Adobe or PowerPoint to Word, etc.). Note: In the system, these are referred to as “Network CIFS Directory.”
- **Structured Data** - Allows monitoring for information stored in databases throughout the organization. Examples could include personnel records, medical records, customer data and more. Note: In the system, these are referred to as “Term Database (CIFS).”
- **Pattern Matching** - Identifies credit card (Visa, MC, AMEX, Discover) numbers and social security numbers as they leave your network. Custom patterns can easily be added as well.
- **Dictionaries** - “Dictionaries” of terms can be defined and scanned. Dictionaries can contain common phrases (such as “confidential and proprietary”), standard industry terms, such as the ICD codes used in healthcare, or terms unique to a particular department or business function.

## Application Firewall

The GV-2010 supports signatures for over 100 content carrying applications such as Facebook, Gmail, BitTorrent, Yahoo, MSN WebMessenger. The institution will be able to monitor application usage trends, highlighting specific applications and their key users. Or, you may decide to block specific application functions. The GV-2010 provides fine-grained intelligent policy enforcement by IP metadata, port metadata and application, supporting monitoring and blocking by discrete application function (such as allow chat and send but block attachments, etc.).

- Increase performance through optimization of specific application traffic
- Reduce costs through optimization of overall application traffic
- Enable new broadband services

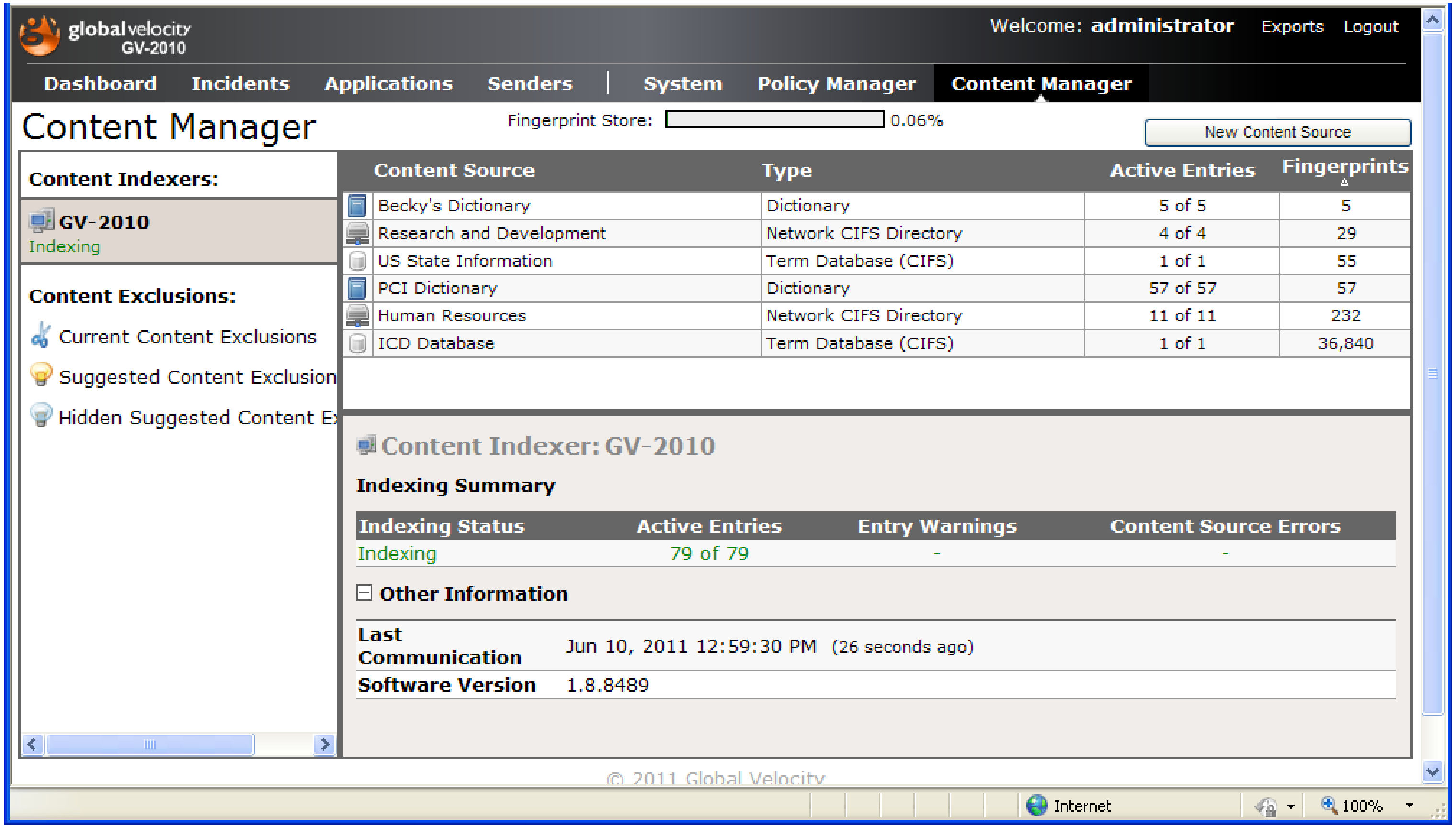
The remainder of this document highlights key capabilities of the system. It is not intended to be a full training document or user guide. The following topics are covered:

- Content Sources
- Policy Manager
- Dashboard
- Importing and exporting policies

## *Sample Content Sources*

In the GV-2010 Content Manager, the defined sample content sources include:

- Two Dictionaries – Becky's Dictionary was created manually while the PCI Dictionary was created using the upload csv file function.
- Two Network CIFS Directories: Network directories that point to folders that contain various types of files such as Excel, Word, PDF and jpeg (unstructured data).
  - **Note:** The R&D directory has 4 files that were fingerprinted while Human Resources folder has 11.
- Two Term Databases: Examples of structured data. These are based on XML files that are manually created or programmatically created from extracted data of a database and converted to XML.
  - **Note:** The ICD database has 36k+ fingerprints while the other content sources are much smaller.



Content Manager

Fingerprint Store: 0.06%

| Content Source | Type | Active Entries | Fingerprints |
|---|---|---|---|
| Becky's Dictionary | Dictionary | 5 of 5 | 5 |
| Research and Development | Network CIFS Directory | 4 of 4 | 29 |
| US State Information | Term Database (CIFS) | 1 of 1 | 55 |
| PCI Dictionary | Dictionary | 57 of 57 | 57 |
| Human Resources | Network CIFS Directory | 11 of 11 | 232 |
| ICD Database | Term Database (CIFS) | 1 of 1 | 36,840 |

Content Indexer: GV-2010

Indexing Summary

| Indexing Status | Active Entries | Entry Warnings | Content Source Errors |
|---|---|---|---|
| Indexing | 79 of 79 | - | - |

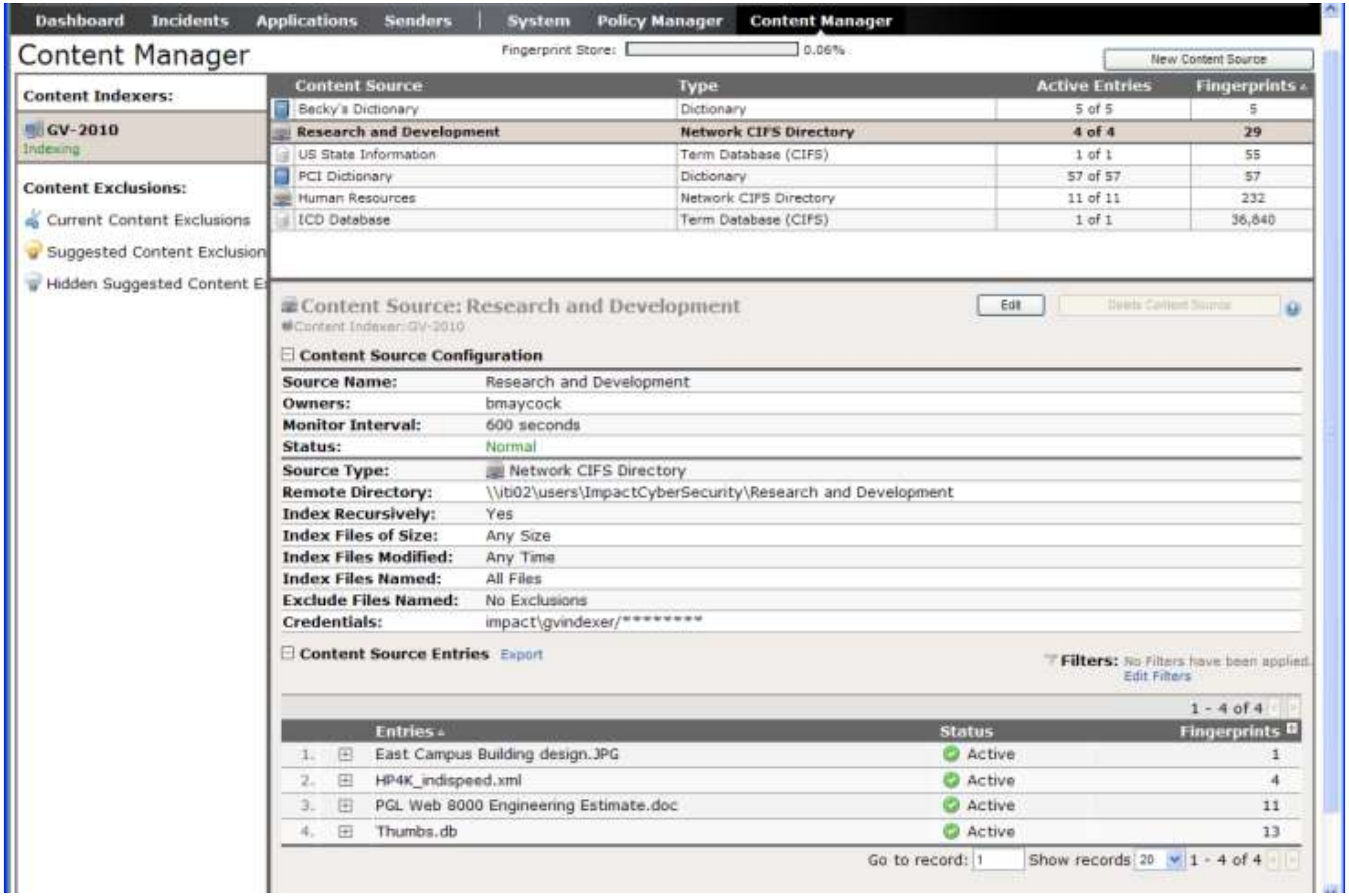
Other Information

| | |
|---|---|
| Last Communication | Jun 10, 2011 12:59:30 PM (26 seconds ago) |
| Software Version | 1.8.8489 |

## *Unstructured Data (Network CIFS Directory)*

Below is a completed sample of a file directory that has been configured to be monitored.

- You define the directory to monitor and provide credentials to access it. You can also set options to limit what is scanned and how often for the GV-2010 to scan.
- At the bottom it outlines which documents are being scanned and shows the number of fingerprints.
- You may have one or more directories defined. You may create users (known as Content Owners) that will be restricted to viewing incidents based on their specific content.



| Content Source | Type | Active Entries | Fingerprints |
|---|---|---|---|
| Becky's Dictionary | Dictionary | 5 of 5 | 5 |
| **Research and Development** | **Network CIFS Directory** | **4 of 4** | **29** |
| US State Information | Term Database (CIFS) | 1 of 1 | 55 |
| PCI Dictionary | Dictionary | 57 of 57 | 57 |
| Human Resources | Network CIFS Directory | 11 of 11 | 232 |
| ICD Database | Term Database (CIFS) | 1 of 1 | 36,840 |

Content Source: Research and Development

Content Indexer: GV-2010

**Content Source Configuration**

| | |
|---|---|
| **Source Name:** | Research and Development |
| **Owners:** | bmaycock |
| **Monitor Interval:** | 600 seconds |
| **Status:** | Normal |
| **Source Type:** | Network CIFS Directory |
| **Remote Directory:** | \\iti02\users\ImpactCyberSecurity\Research and Development |
| **Index Recursively:** | Yes |
| **Index Files of Size:** | Any Size |
| **Index Files Modified:** | Any Time |
| **Index Files Named:** | All Files |
| **Exclude Files Named:** | No Exclusions |
| **Credentials:** | impact\gvindexer/******** |

**Content Source Entries** Export

**Filters:** No Filters have been applied.
Edit Filters

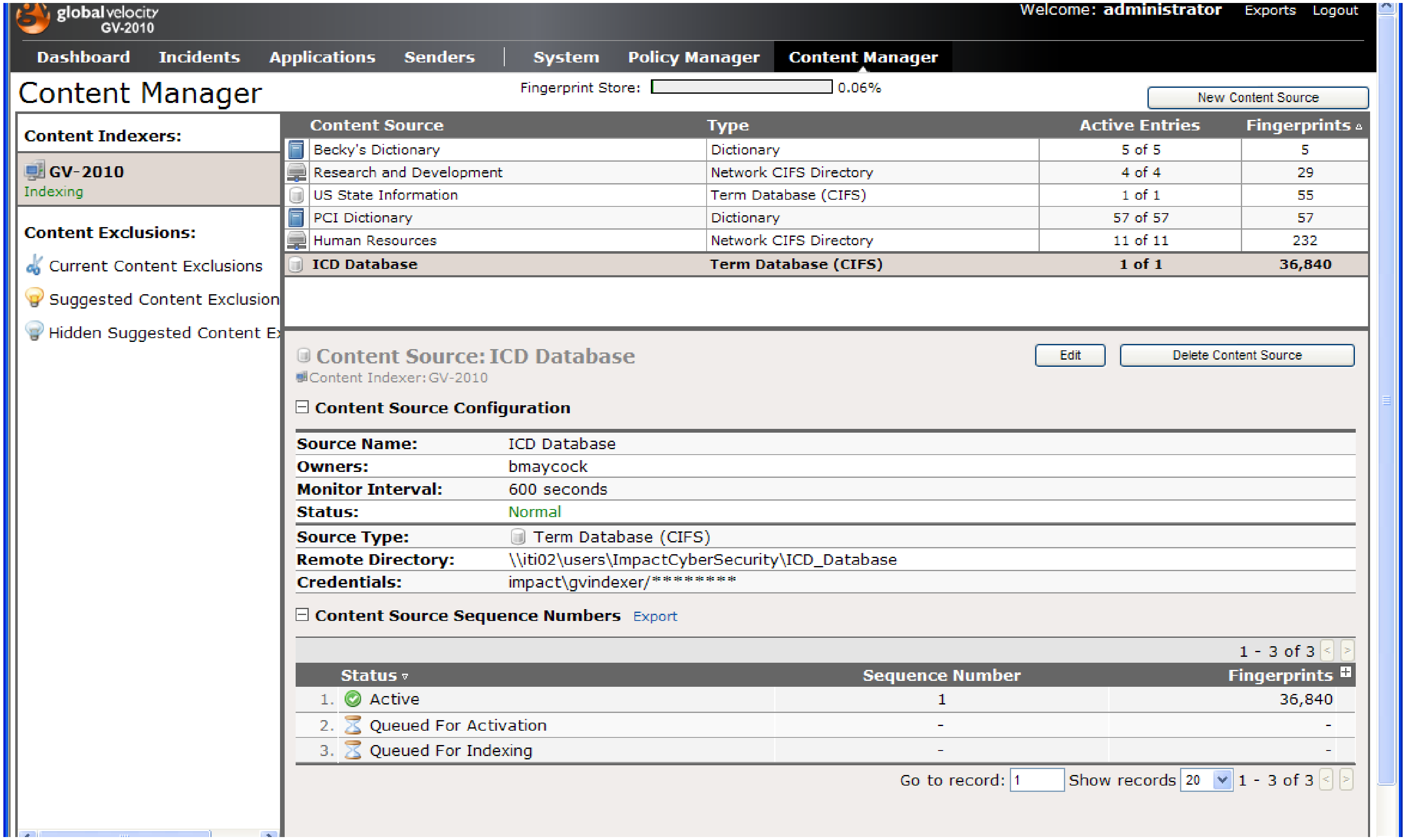
1 - 4 of 4

| | Entries | Status | Fingerprints |
|---|---|---|---|
| 1. | East Campus Building design.JPG | Active | 1 |
| 2. | HP4K_indispeed.xml | Active | 4 |
| 3. | PGL Web 8000 Engineering Estimate.doc | Active | 11 |
| 4. | Thumbs.db | Active | 13 |

Go to record: 1 Show records 20 1 - 4 of 4

## *Structured Data (Term Database (CIFS))*

Below you can see a completed content source configuration screen for a database. This is very similar to the Network CIFS because it simply points to XML document(s).



| Content Source | Type | Active Entries | Fingerprints |
|---|---|---|---|
| Becky's Dictionary | Dictionary | 5 of 5 | 5 |
| Research and Development | Network CIFS Directory | 4 of 4 | 29 |
| US State Information | Term Database (CIFS) | 1 of 1 | 55 |
| PCI Dictionary | Dictionary | 57 of 57 | 57 |
| Human Resources | Network CIFS Directory | 11 of 11 | 232 |
| **ICD Database** | **Term Database (CIFS)** | **1 of 1** | **36,840** |

**Content Source: ICD Database**

Content Indexer: GV-2010

⊟ **Content Source Configuration**

| | |
|---|---|
| **Source Name:** | ICD Database |
| **Owners:** | bmaycock |
| **Monitor Interval:** | 600 seconds |
| **Status:** | Normal |
| **Source Type:** | Term Database (CIFS) |
| **Remote Directory:** | \\iti02\users\ImpactCyberSecurity\ICD_Database |
| **Credentials:** | impact\gvindexer/********* |

⊟ **Content Source Sequence Numbers** Export

1 - 3 of 3

| | Status | Sequence Number | Fingerprints |
|---|---|---|---|
| 1. | ✓ Active | 1 | 36,840 |
| 2. | Queued For Activation | - | - |
| 3. | Queued For Indexing | - | - |

Go to record: 1 Show records 20 1 - 3 of 3

### *More About Structured Data*

Let’s start with a few definitions:

1. **Field** – Relational databases arrange data as sets of database records, also called rows. Each record consists of several fields; the fields of all records form the columns.  Data that has several parts can be divided into fields.
2. **Term** – A value to be indexed.  Terms are differentiated from fields as several fields may be concatenated in various orders to produce terms.  For example, the fields LastName, FirstName, and MiddleInitial may be used to create three terms for indexing:
   a. Term 1 – LastName, FirstName, MiddleInitial
   b. Term 2 – LastName, FirstName
   c. Term 3 – FirstName, LastName
3. **Weight** – A value of importance, as determined by the data owner, assigned to each term.  The value can be tuned higher for more sensitive information or can be tuned lower to decrease the probability of false positives.
4. **Accumulated Weight** – The accumulation of weights for terms seen in a flow.  When this value reaches a set threshold or above, a match is declared and an Incident is created by the GV-2010.
5. **Threshold** – A system-wide value that is set by the Administrator that determines the value at which an Accumulated Weight for a flow will create an incident.

At a high level, the following steps are key for creating a structured data source:

- Determine what information in the database needs to be protected and in what configuration / format to define Terms.
- Determine a weight for each term.
- Design an extract to obtain the information, assign the defined weight and output in the XML format required by the GV-2010 Indexer. This process would likely be automated and execute at a pre-set frequency to accommodate changes in the source data.
- Define the content source in the web interface to point to the XML file(s).

Below is the beginning of a sample XML file.  Python is the programming language that some of the Global Velocity team likes to use to generate the XML documents.

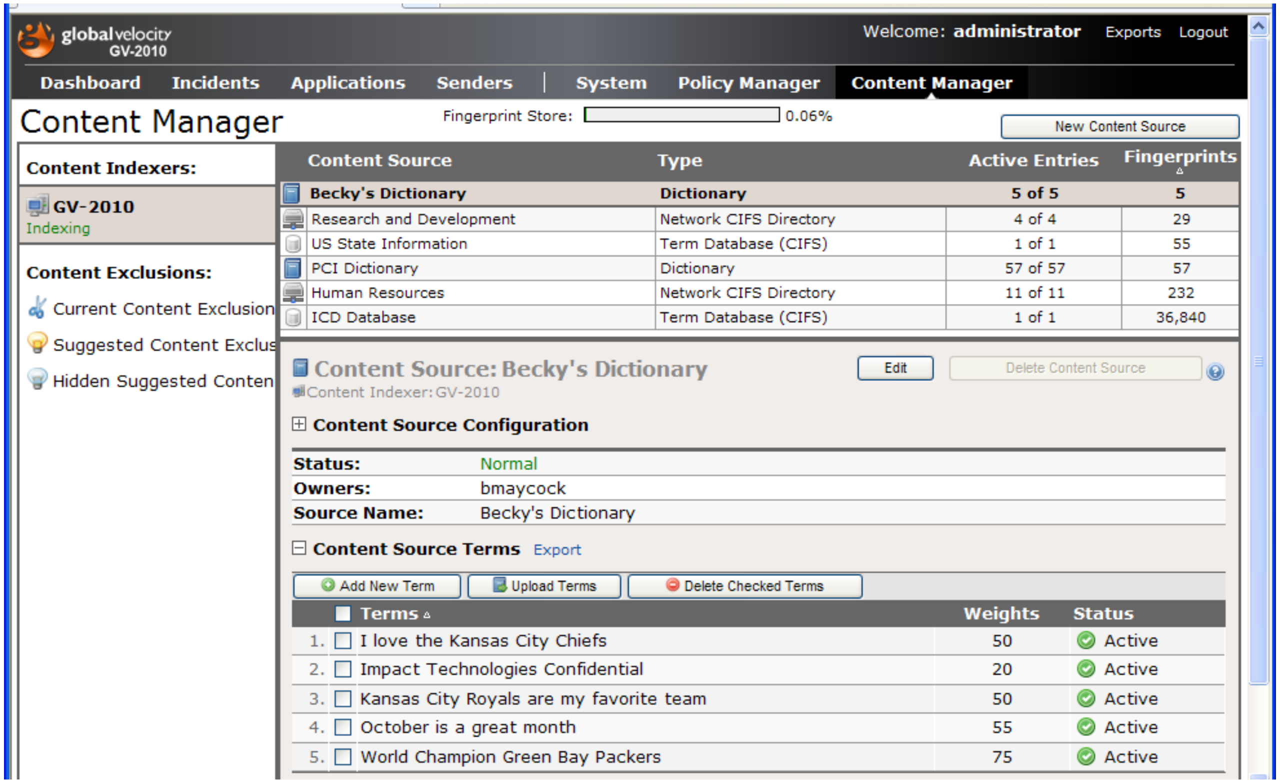
```
<?xml version="1.0" encoding="UTF-8"?>
<GV2000_CONFIG>
<term string="AAT deficiency" weight="10" op="add" />
<term string="abacterial" weight="10" op="add" />
<term string="abdominal" weight="10" op="add" />
<term string="Abdominal distention (gaseous)" weight="10" op="add" />
<term string="Abdominal heart" weight="10" op="add" />
<term string="Abdominal migraine" weight="10" op="add" />
<term string="abdominal NOS" weight="10" op="add" />
```

## Dictionary

Below you can see a completed content source configuration screen for “Becky’s Dictionary.” This is the simplest method if there are key terms you want to scan. You can use the “Add New Term” and manually enter new terms. Or, create a csv file and use the “Upload Terms” option. Format for csv file is simply: “term, weight” such as:

```
Account,3
Address,10
Billing,10
Payment,10
123.123, 10
```

***Note:** the fingerprinting process effectively strips out punctuation and spaces, but it does use it to “match” the length of the dictionary term. So, “123.123” will match “123.123”, “123-123”, 12.3123 and “123123”, but it won’t match “123123123”. The dictionaries are actually a special case of the XML-based structured content, so from a fingerprinting standpoint they work exactly the same.*



Content Manager

Fingerprint Store: 0.06%

Content Indexers:

GV-2010
Indexing

Content Exclusions:

- Current Content Exclusion
- Suggested Content Exclus
- Hidden Suggested Conten

| Content Source | Type | Active Entries | Fingerprints |
|---|---|---|---|
| Becky's Dictionary | Dictionary | 5 of 5 | 5 |
| Research and Development | Network CIFS Directory | 4 of 4 | 29 |
| US State Information | Term Database (CIFS) | 1 of 1 | 55 |
| PCI Dictionary | Dictionary | 57 of 57 | 57 |
| Human Resources | Network CIFS Directory | 11 of 11 | 232 |
| ICD Database | Term Database (CIFS) | 1 of 1 | 36,840 |

Content Source: Becky's Dictionary
Content Indexer: GV-2010

⊞ Content Source Configuration

| | |
|---|---|
| **Status:** | Normal |
| **Owners:** | bmaycock |
| **Source Name:** | Becky's Dictionary |

⊟ Content Source Terms

| | □ Terms | Weights | Status |
|---|---|---|---|
| 1. | □ I love the Kansas City Chiefs | 50 | ✓ Active |
| 2. | □ Impact Technologies Confidential | 20 | ✓ Active |
| 3. | □ Kansas City Royals are my favorite team | 50 | ✓ Active |
| 4. | □ October is a great month | 55 | ✓ Active |
| 5. | □ World Champion Green Bay Packers | 75 | ✓ Active |

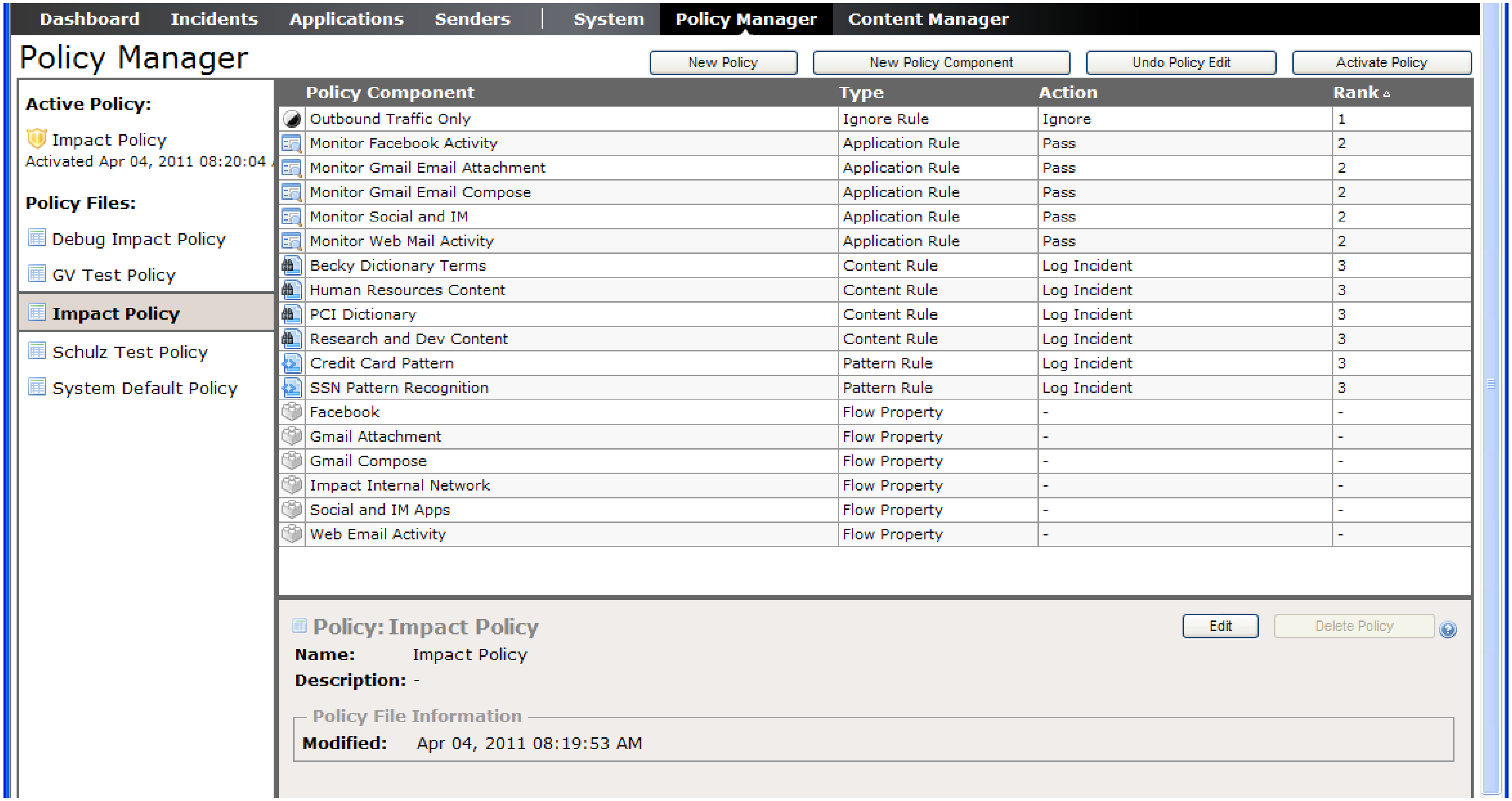
## Pattern Matching

To search for credit cards and social security numbers leaving the network, you do not need to set up a content source. You simply create a policy as discussed in the next section.

## *Policy Manager*

The GV-2010 allows you to create Policy Files. You may create several but only one is active at a time. The Impact Policy below has many policy components that mix pattern matching, content rules and application rules. The basic structure is that you create a “flow property” that defines the traffic you want to look at (such as by IP range, port or application) and then you can create the Application Rule or Content Rule that you want to apply to that traffic.

- You can see several Application Rules that monitor for different types of application signatures, some more granular than others.
- Then you see the list of content and pattern matching rules.



Policy Manager

**Active Policy:**

Impact Policy
Activated Apr 04, 2011 08:20:04

**Policy Files:**

Debug Impact Policy
GV Test Policy
**Impact Policy**
Schulz Test Policy
System Default Policy

| Policy Component | Type | Action | Rank |
|---|---|---|---|
| Outbound Traffic Only | Ignore Rule | Ignore | 1 |
| Monitor Facebook Activity | Application Rule | Pass | 2 |
| Monitor Gmail Email Attachment | Application Rule | Pass | 2 |
| Monitor Gmail Email Compose | Application Rule | Pass | 2 |
| Monitor Social and IM | Application Rule | Pass | 2 |
| Monitor Web Mail Activity | Application Rule | Pass | 2 |
| Becky Dictionary Terms | Content Rule | Log Incident | 3 |
| Human Resources Content | Content Rule | Log Incident | 3 |
| PCI Dictionary | Content Rule | Log Incident | 3 |
| Research and Dev Content | Content Rule | Log Incident | 3 |
| Credit Card Pattern | Pattern Rule | Log Incident | 3 |
| SSN Pattern Recognition | Pattern Rule | Log Incident | 3 |
| Facebook | Flow Property | - | - |
| Gmail Attachment | Flow Property | - | - |
| Gmail Compose | Flow Property | - | - |
| Impact Internal Network | Flow Property | - | - |
| Social and IM Apps | Flow Property | - | - |
| Web Email Activity | Flow Property | - | - |

Policy: Impact Policy

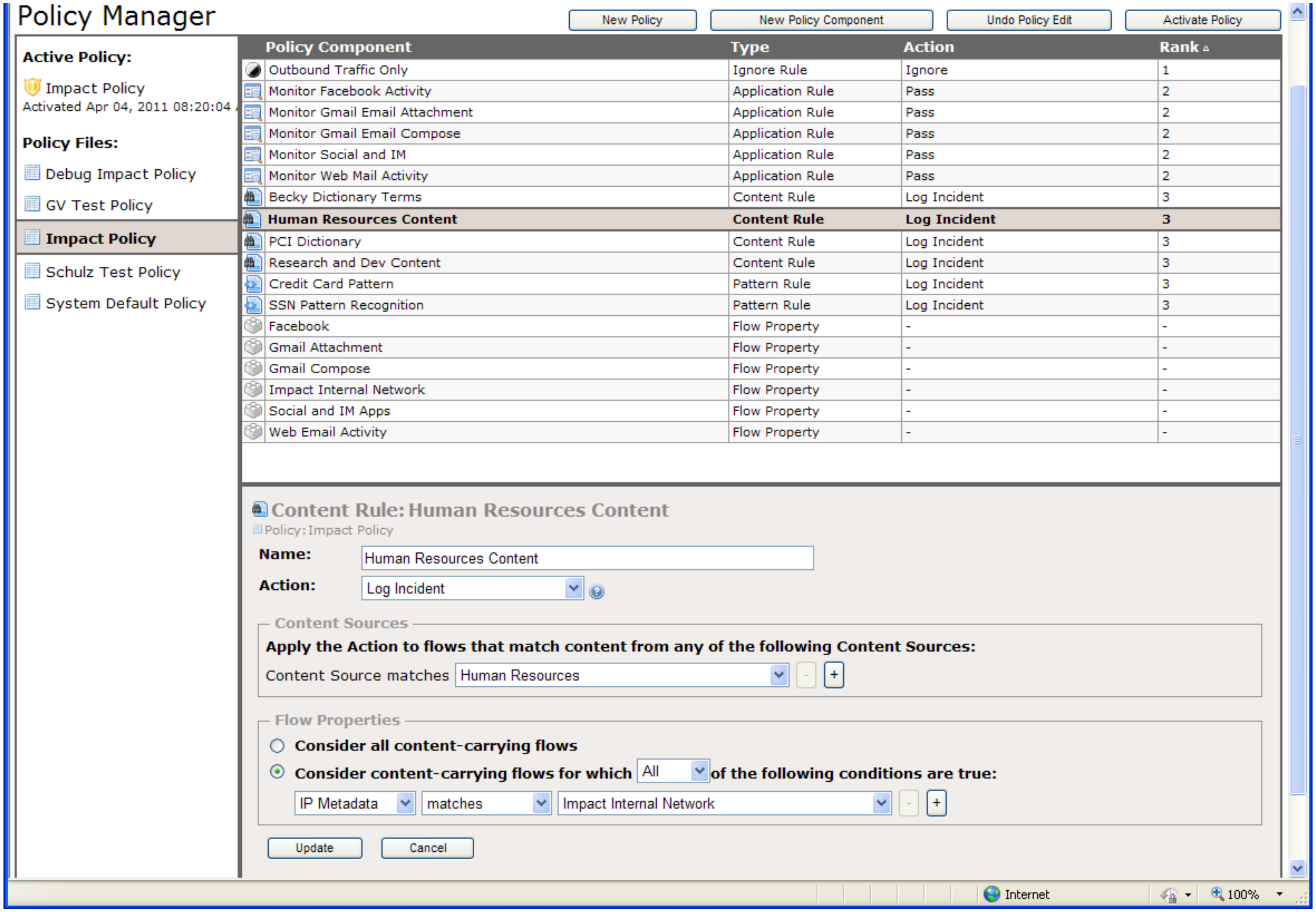
**Name:** Impact Policy
**Description:** -

Policy File Information

**Modified:** Apr 04, 2011 08:19:53 AM

Below you can see the details for the Human Resources Content policy component.

- Give it a name and set the action (Log incident).
- Point to the content source that has been previously defined.
- Associate the Flow properties that are applicable (what traffic do you want the GV-2010 to monitor for this type of content).



Policy Manager

**Active Policy:**

Impact Policy
Activated Apr 04, 2011 08:20:04

**Policy Files:**

- Debug Impact Policy
- GV Test Policy
- **Impact Policy**
- Schulz Test Policy
- System Default Policy

| Policy Component | Type | Action | Rank |
|---|---|---|---|
| Outbound Traffic Only | Ignore Rule | Ignore | 1 |
| Monitor Facebook Activity | Application Rule | Pass | 2 |
| Monitor Gmail Email Attachment | Application Rule | Pass | 2 |
| Monitor Gmail Email Compose | Application Rule | Pass | 2 |
| Monitor Social and IM | Application Rule | Pass | 2 |
| Monitor Web Mail Activity | Application Rule | Pass | 2 |
| Becky Dictionary Terms | Content Rule | Log Incident | 3 |
| **Human Resources Content** | **Content Rule** | **Log Incident** | **3** |
| PCI Dictionary | Content Rule | Log Incident | 3 |
| Research and Dev Content | Content Rule | Log Incident | 3 |
| Credit Card Pattern | Pattern Rule | Log Incident | 3 |
| SSN Pattern Recognition | Pattern Rule | Log Incident | 3 |
| Facebook | Flow Property | - | - |
| Gmail Attachment | Flow Property | - | - |
| Gmail Compose | Flow Property | - | - |
| Impact Internal Network | Flow Property | - | - |
| Social and IM Apps | Flow Property | - | - |
| Web Email Activity | Flow Property | - | - |

**Content Rule: Human Resources Content**

Policy: Impact Policy

**Name:** Human Resources Content

**Action:** Log Incident

Content Sources

**Apply the Action to flows that match content from any of the following Content Sources:**

Content Source matches Human Resources

Flow Properties

○ **Consider all content-carrying flows**

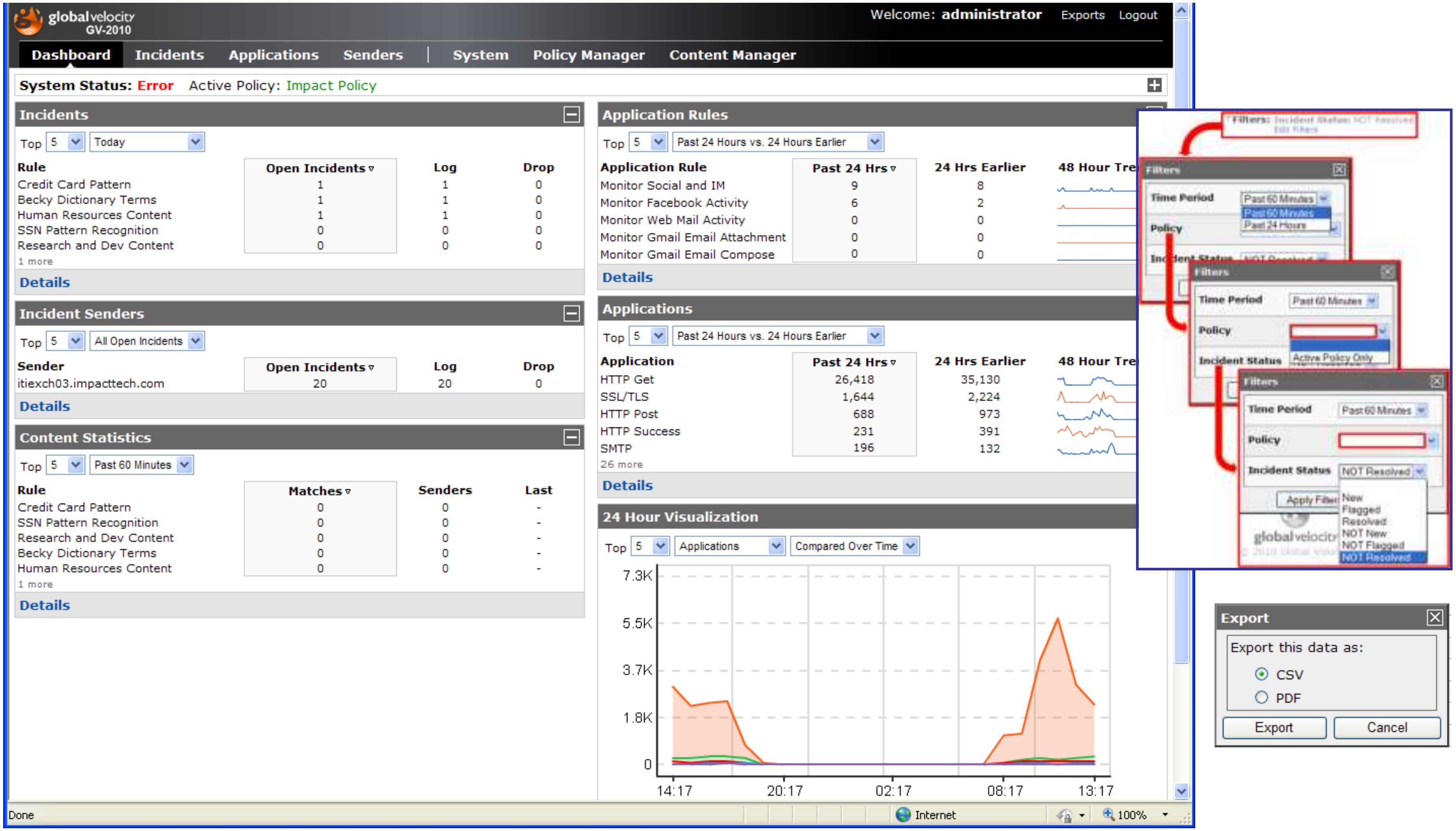
● **Consider content-carrying flows for which** All **of the following conditions are true:**

IP Metadata matches Impact Internal Network

Update Cancel

## Dashboard

The Dashboard provides a quick reference to all the content policy and application rules that are defined. In the Incidents, you not only see the pattern matching incidents (such as CC and SSN) but you also see the Dictionary and Content incidents. On the right, are the breakout of the specific application signatures rules in addition to the application usage. When viewing Incidents and Applications, you can use the filters to distill the information and then export to csv or PDF. (Ignore the error status. The second power supply was temporarily unplugged.)



System Status: Error Active Policy: Impact Policy

**Incidents**

Top 5 Today

| Rule | Open Incidents ▿ | Log | Drop |
|---|---|---|---|
| Credit Card Pattern | 1 | 1 | 0 |
| Becky Dictionary Terms | 1 | 1 | 0 |
| Human Resources Content | 1 | 1 | 0 |
| SSN Pattern Recognition | 0 | 0 | 0 |
| Research and Dev Content | 0 | 0 | 0 |

1 more

Details

**Incident Senders**

Top 5 All Open Incidents

| Sender | Open Incidents ▿ | Log | Drop |
|---|---|---|---|
| itiexch03.impacttech.com | 20 | 20 | 0 |

Details

**Content Statistics**

Top 5 Past 60 Minutes

| Rule | Matches ▿ | Senders | Last |
|---|---|---|---|
| Credit Card Pattern | 0 | 0 | - |
| SSN Pattern Recognition | 0 | 0 | - |
| Research and Dev Content | 0 | 0 | - |
| Becky Dictionary Terms | 0 | 0 | - |
| Human Resources Content | 0 | 0 | - |

1 more

Details

**Application Rules**

Top 5 Past 24 Hours vs. 24 Hours Earlier

| Application Rule | Past 24 Hrs ▿ | 24 Hrs Earlier | 48 Hour Tre |
|---|---|---|---|
| Monitor Social and IM | 9 | 8 | |
| Monitor Facebook Activity | 6 | 2 | |
| Monitor Web Mail Activity | 0 | 0 | |
| Monitor Gmail Email Attachment | 0 | 0 | |
| Monitor Gmail Email Compose | 0 | 0 | |

Details

**Applications**

Top 5 Past 24 Hours vs. 24 Hours Earlier

| Application | Past 24 Hrs ▿ | 24 Hrs Earlier | 48 Hour Tre |
|---|---|---|---|
| HTTP Get | 26,418 | 35,130 | |
| SSL/TLS | 1,644 | 2,224 | |
| HTTP Post | 688 | 973 | |
| HTTP Success | 231 | 391 | |
| SMTP | 196 | 132 | |

26 more

Details

**24 Hour Visualization**

Top 5 Applications Compared Over Time

Filters: Incident Status: NOT Resolved
Edit Filters

**Filters**

Time Period: Past 60 Minutes (Past 60 Minutes / Past 24 Hours)
Policy:
Incident Status: NOT Resolved

**Filters**

Time Period: Past 60 Minutes
Policy: (Active Policy Only)
Incident Status

**Filters**

Time Period: Past 60 Minutes
Policy:
Incident Status: NOT Resolved (New / Flagged / Resolved / NOT New / NOT Flagged / NOT Resolved)

**Export**

Export this data as:

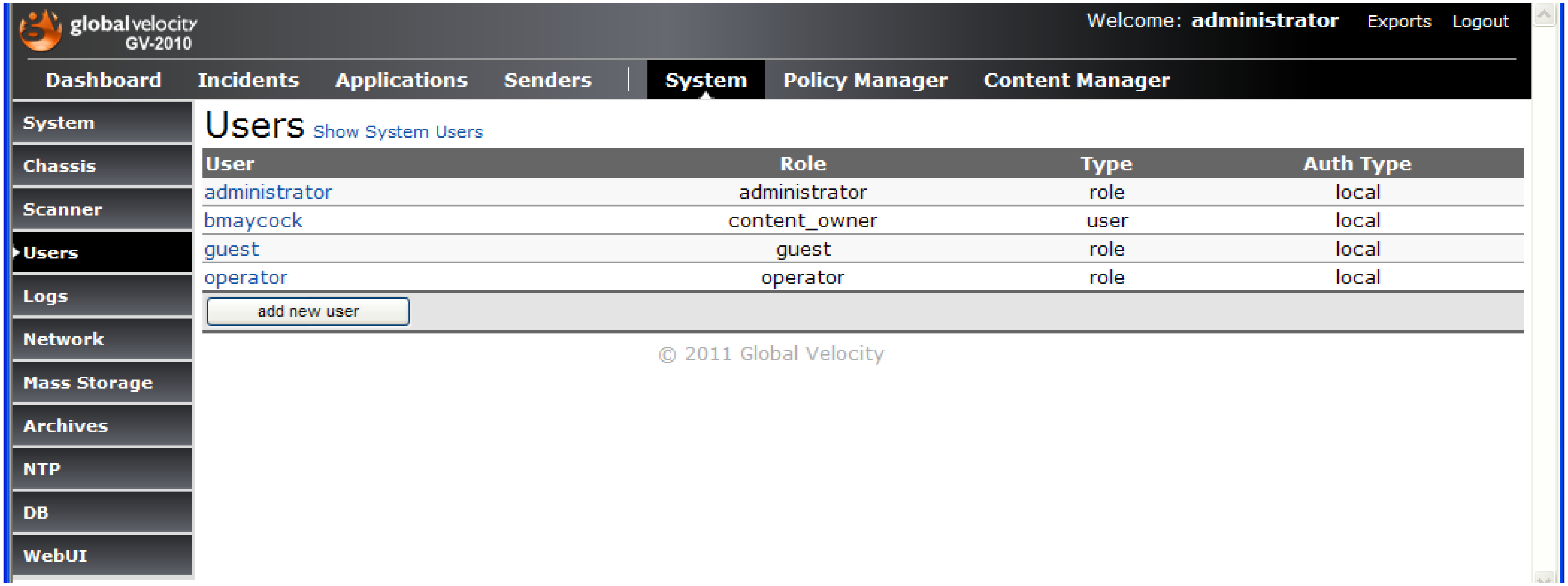
● CSV
○ PDF

## System

The System tabs contain important information about the status of the system. You can also see information concerning the chassis, scanner, users, logs, network, mass storage, NTP, DB, and WebUI.

### Users

Select the Users tab to see the list of users. For each user the user name, role, type and auth type are listed. The fields are hyperlinked to a page which details definition for that user. From the user page, you can go to a page to add a new user.



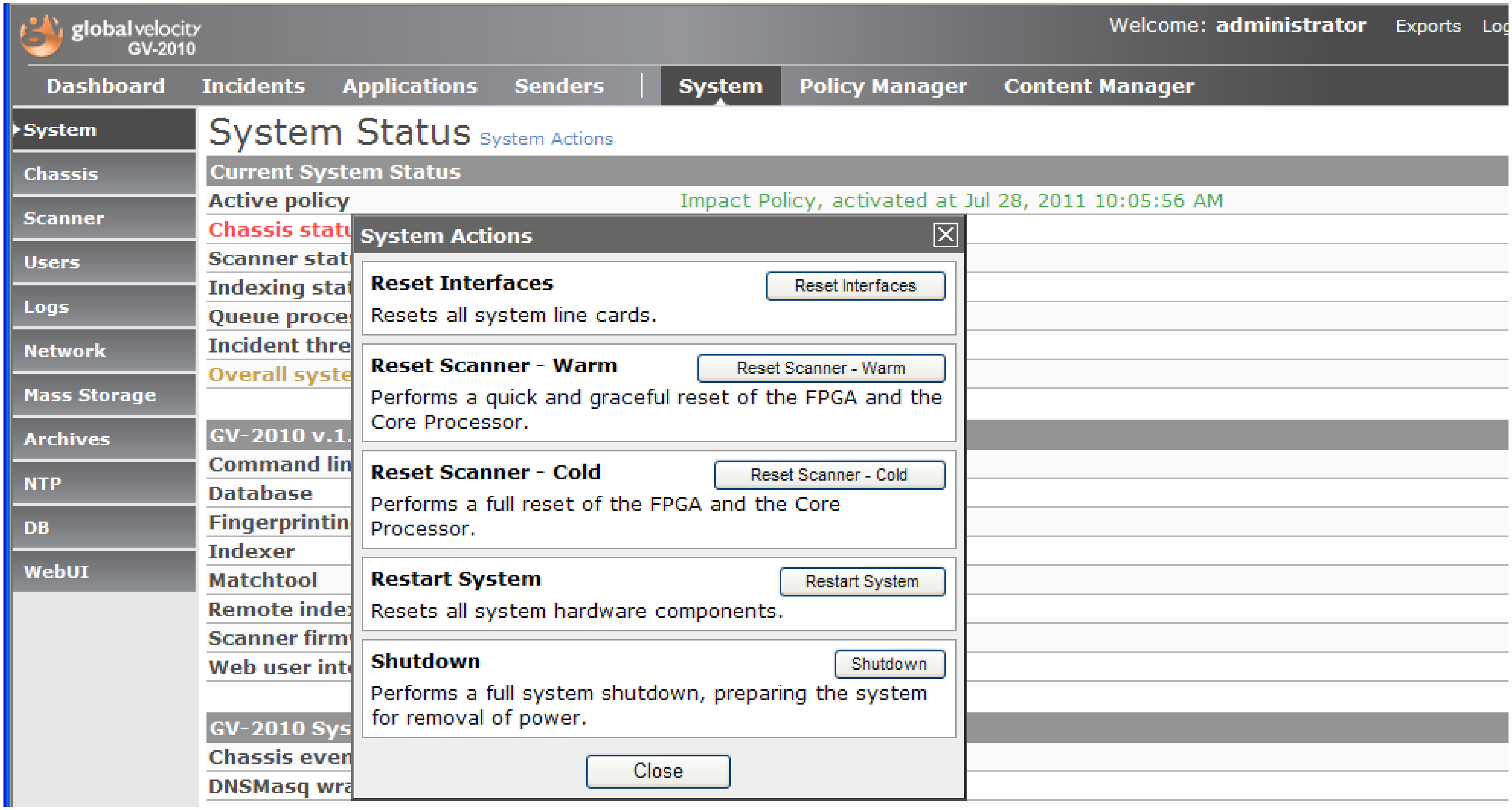
Users Show System Users

| User | Role | Type | Auth Type |
|---|---|---|---|
| administrator | administrator | role | local |
| bmaycock | content_owner | user | local |
| guest | guest | role | local |
| operator | operator | role | local |

© 2011 Global Velocity

### *System Actions*

From the main System page, click on the System Actions link to access the reset scanner and shutdown options.  Refer to the GV-2010 Troubleshooting Guide for more information.



Active policy: Impact Policy, activated at Jul 28, 2011 10:05:56 AM

**Reset Interfaces**
Resets all system line cards.

**Reset Scanner - Warm**
Performs a quick and graceful reset of the FPGA and the Core Processor.

**Reset Scanner - Cold**
Performs a full reset of the FPGA and the Core Processor.

**Restart System**
Resets all system hardware components.

**Shutdown**
Performs a full system shutdown, preparing the system for removal of power.

## *Importing/Exporting Policies*

Below is an outline of exporting a policy from one GV-2010 and importing it into another.

### *Exporting*

- Log into the device using secure FTP (SFTP, Filezilla, etc). The default user/pass is ftpuser/ftp
- cd to the policy directory
- Get the desired policy file

### *Importing*

- Log into the device using secure FTP
- cd to the upload directory
- Put the desired policy file
- From the Policy Manager WebUI, click the “New Policy” button, and click the name of the policy file under “Import Policy File”