Websense Data Security 7.7

New Features and Best Practices

TRITON™

- Web security
- Email security
- Data security
- Mobile security

Operating system support

- TRITON management server
  - Windows 2008 R2 only
- Supplemental Data Security servers
  - Same as v7.6
  - Windows 2003 R2 (32bit)
  - Windows 2008 R2
- Data Security agents
  - Same as v7.6
  - Crawler
    - Windows 2003 R2 32bit
    - Windows 2008 R2 64bit
  - Printer agent
    - Windows 2003 (& R2) 32bit
  - ISA\TMG Agent
    - Windows 2003 (& R2) 32bit
    - Windows 2008 R2 64bit
  - SMTP Agent
    - Windows 2003 (& R2) – 32bit and 64bit (with no Policy Engine)

Upgrade

- The 7.7 upgrade is a simple installer-based upgrade (as opposed to the export/import process in 7.5→7.6)
- Servers
  - Management server
    - TRITON unified installer
    - 7.6.x → 7.7
    - If you're upgrading the OS, system backup and restore is needed. You can either 1) upgrade the system in place and backup the upgraded setup or 2) backup the current 7.6.x setup, restore it on the new OS, and upgrade it to 7.7.
  - Data Security servers
    - 7.6.x → 7.7
  - Protector
    - 7.6→7.7
- Endpoints
  - 7.6.x → 7.7
  - Backward compatibility:
    - Incidents are still reported to the 7.7 management server
    - The entire endpoint profile can be switched to "monitoring only" mode (Settings → Endpoint → Settings → Upgrade)

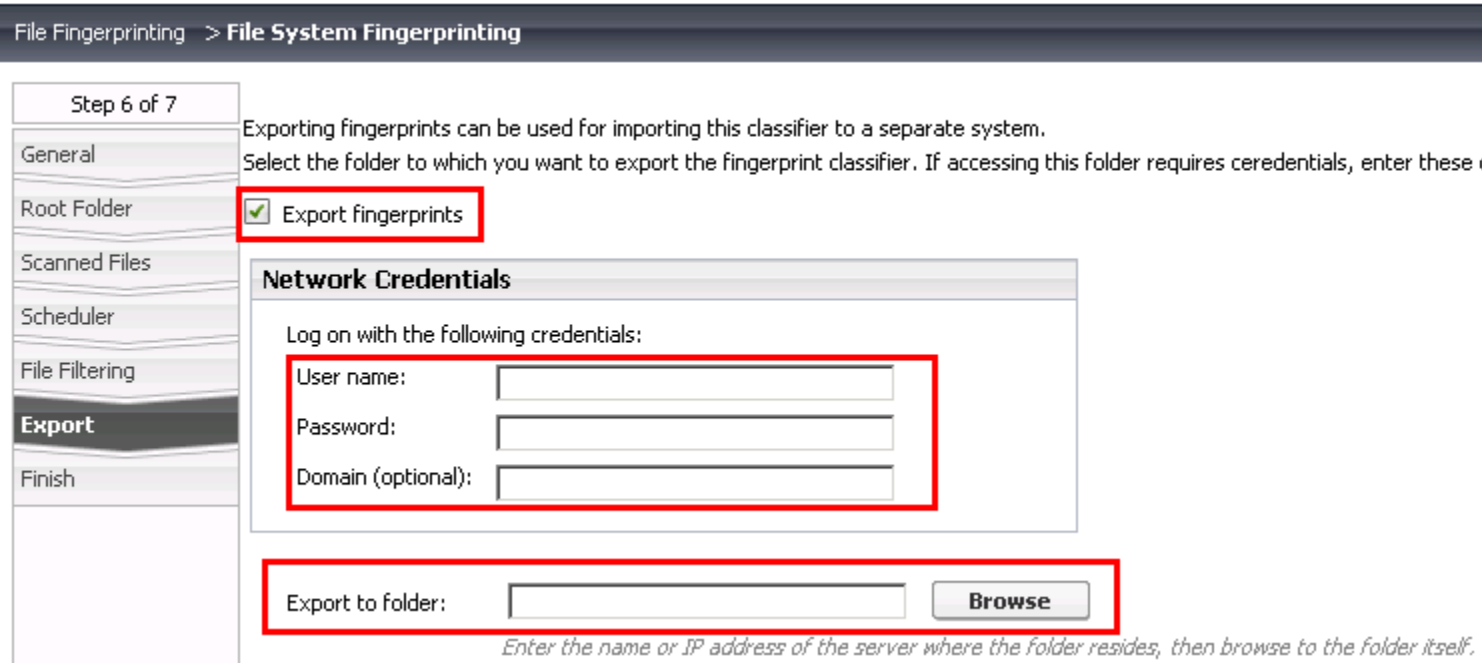
New features

- Fingerprint repository sync over disconnected networks
- High availability / failover
  - Support SQL high-availability solution (cluster)
  - Support management server failover
- Supervised machine learning
- Incident escalation improvements
- OCR capabilities
- Email-based incident workflow management
- Network communication ports consolidation
- Resource resolver optimizations for large user directories
- Cumulative DLP
- Proprietary Excel and Word 2007/2010 extractors
- LDAP attributes enhancements
  - Incidents and reporting
  - Policy creation
- Advanced Persistent Threat protection

FPR sync over disconnected networks

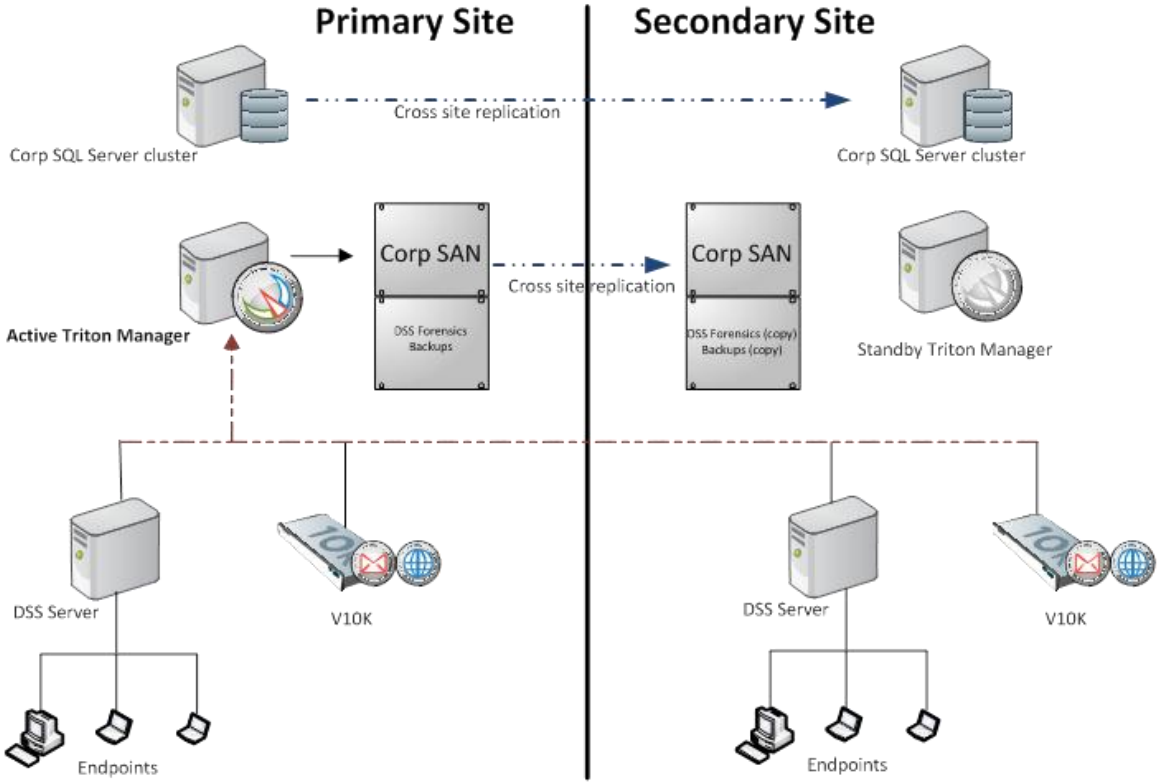
- FPR = fingerprint repository
- Feature request driven by customer requests (mostly government/military)
- Beneficial for customers who have 2 or more separate networks—for example, “internal” and “top secret”—where there’s a need to protect top secret content on the internal network where there’s no actual access to these files
- Introduces ability to export fingerprints created by a classifier on one manager and import them as a new classifier to another manager
- Requires 2 separate v7.7 management servers
- More detailed information can be found here: http://www.websense.com/content/support/library/data/v77/help/Ch%2010-Define%20Content.13.55.aspx

FPR sync over disconnected networks



High availability / failover

- Active-Passive managers
- Based on backup\restore functionality
- Once restore is done, “deploy settings” routes all Data Security servers to the new manager



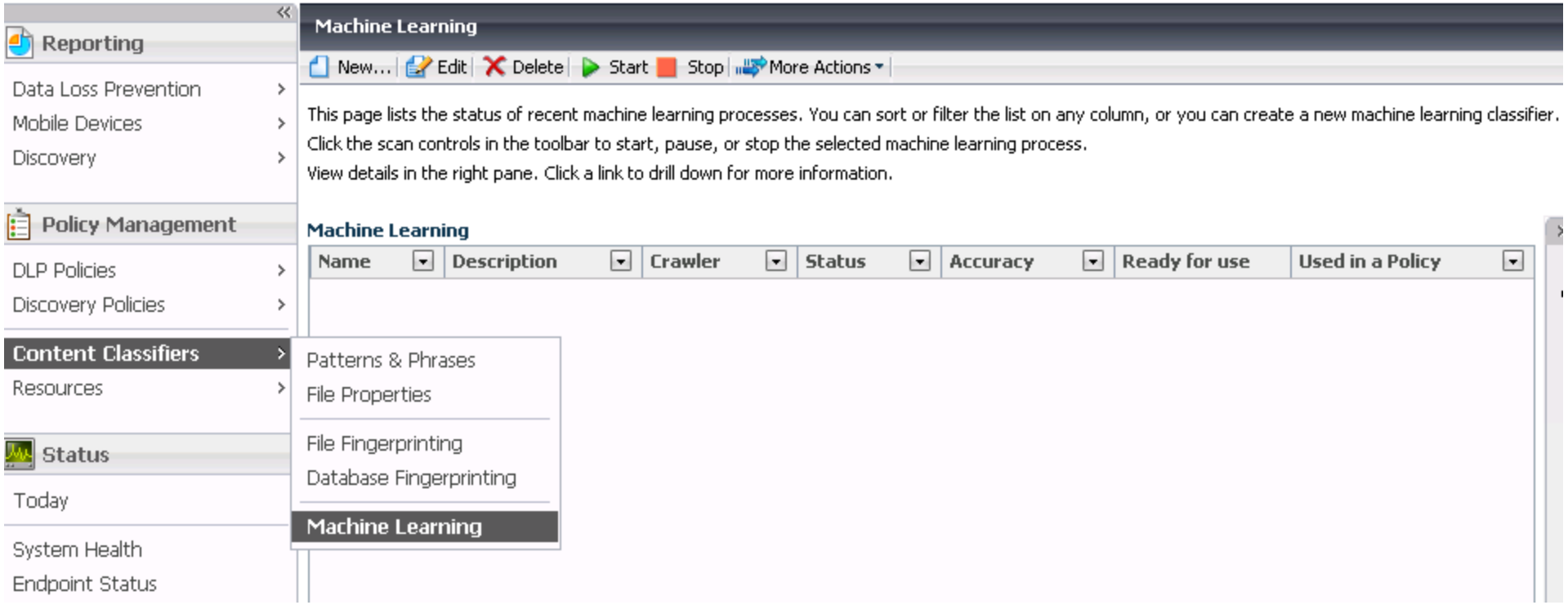
Supervised Machine Learning

websense

- Introduces ability to “learn” the characteristics of a similar set of documents—for example, financial documents of a specific company
- Unlike fingerprints, any new document that are created (financial documents in this example) are protected
- Positive and negative examples must be provided to “train” the classifier
- More detailed information is available here: http://www.websense.com/content/support/library/data/v77/help/mach_learning.aspx and here: http://www.websense.com/content/support/library/data/tips/machine_learning/Introduction%20to%20machine%20learning.pdf

Supervised Machine Learning

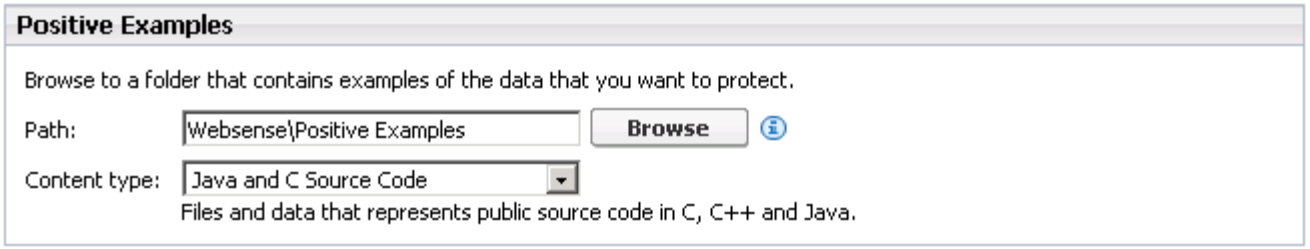
websense



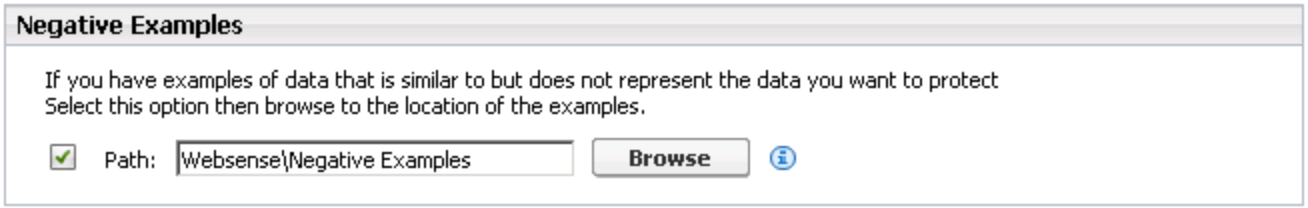
Supervised Machine Learning

websense

- Positive Examples



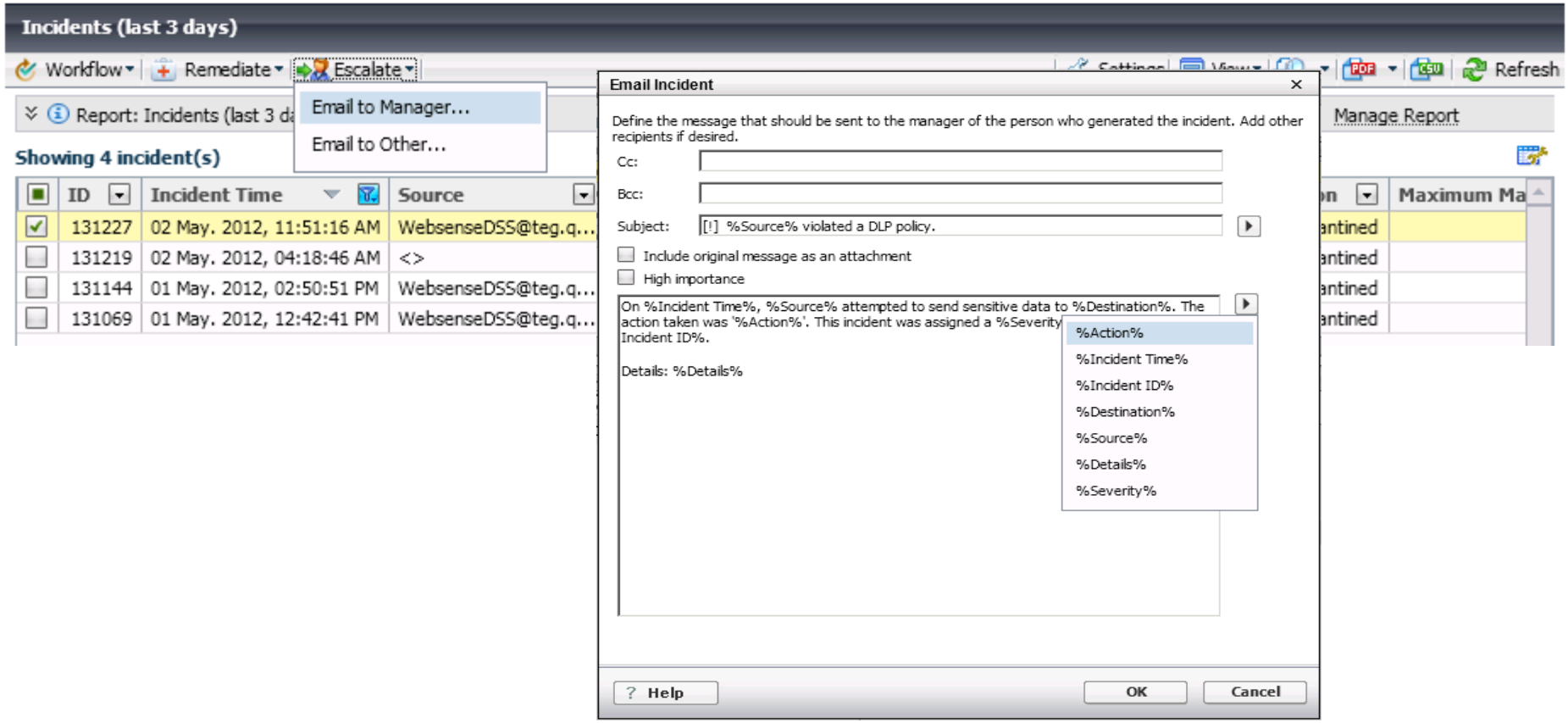
- Negative Examples



- All Documents (optional)

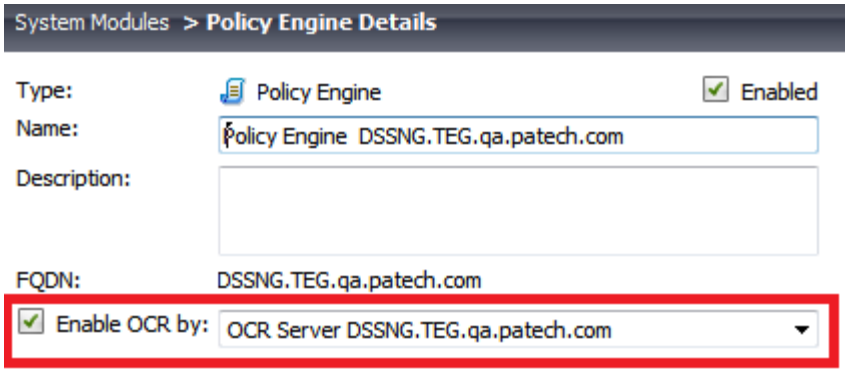
Incident escalation improvements

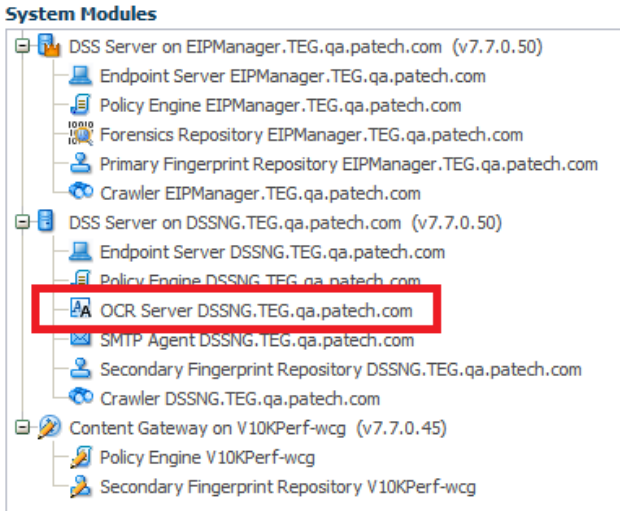
- System variables and default text for the incident email escalation operation



Optical Character Recognition

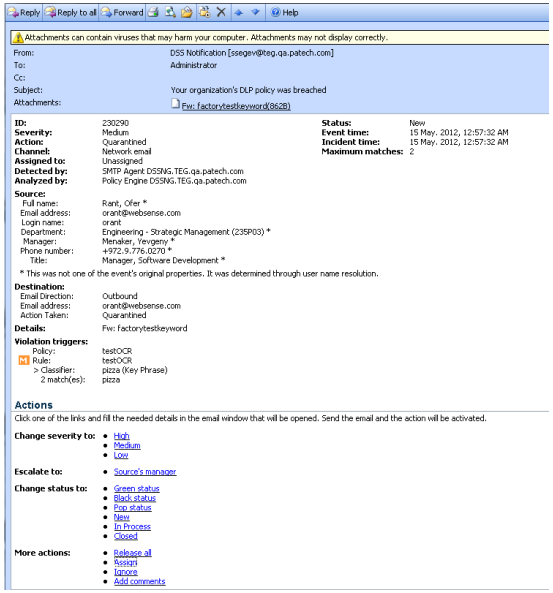
- Added OCR capabilities for text extraction from images containing text (scanned documents, for example)
- Applies to network email, discovery, and Web channels only
- Can be installed only on secondary Windows Data Security servers
- Filter in the Policy Engine decides which images should go through OCR text extraction





Email-based incident workflow management

- Email notifications can now include actions (links in the notification message) that administrators can do without logging into the TRITON Console
- When an administrator clicks an action, a new message is opened with a workflow code
- This email is sent to a system mailbox
- Tomcat periodically checks for new action messages in the system mailbox and operates according to the workflow code
- POP3\IMAP is used
- Force release is still supported in the previous format



Network communication port consolidation

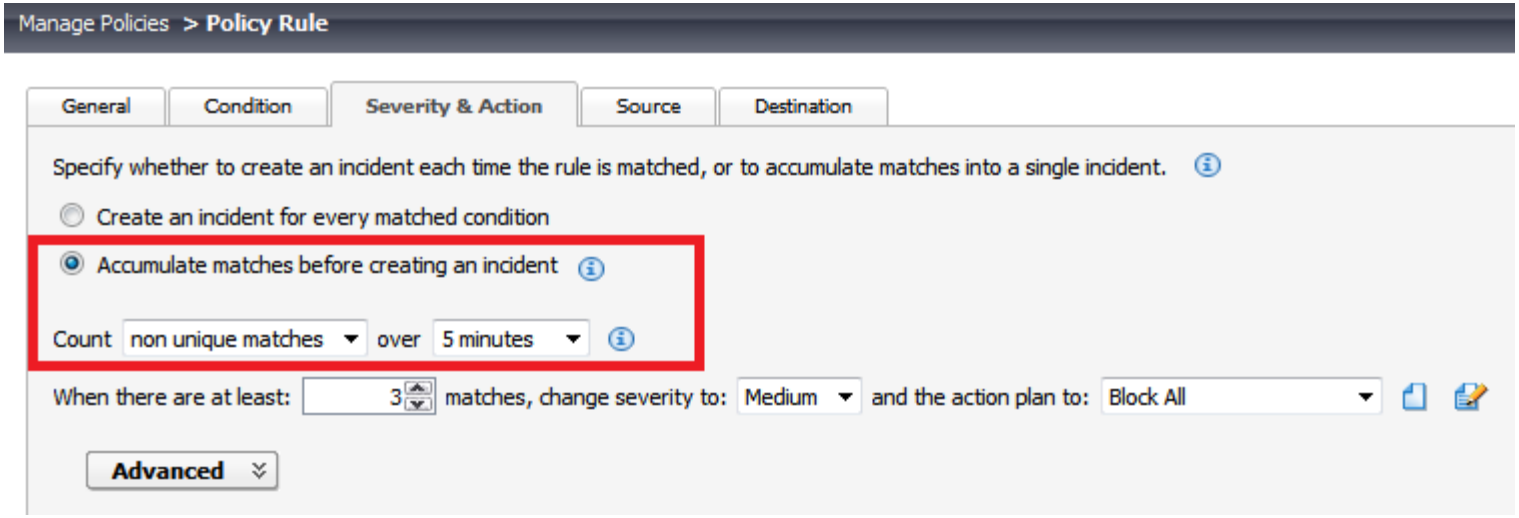
- Most ports are now in consecutive numbering (starting 17500 by default ending at 17515)
  - You must configure your firewall to leave these ports open
- Added ability to configure the port's range beginning
  - This can be done during installation
- Configuration can be done per Data Security server

Resource resolver improvements

- Improved support for large user directory imports
- Tested up to 400,000 objects
- Significant resource resolver database creation performance improvements
- Significant reduction in system resources utilization (CPU, memory, disk) during resource resolver database creation

Cumulative DLP policies

- Detection of data leaks over time (for example, 10 CCNs total from the same source in a 3-day time period)
- Feature existed in 7.6.x for specific rules, but is now available in the TRITON Console and can be configured for every rule



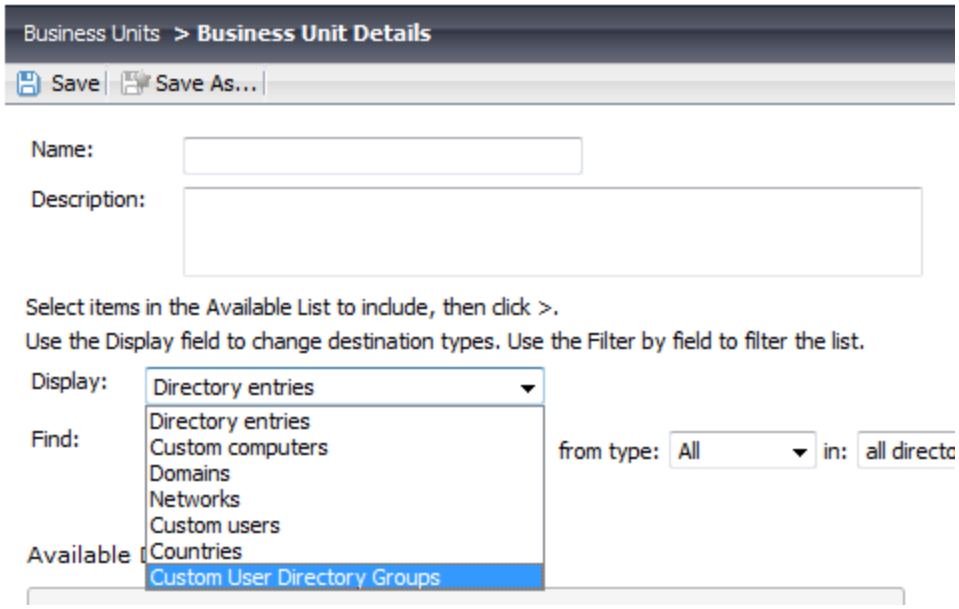
Proprietary Excel and Word extractors

websense

- Improves “mega breaches” detection
- Applies to Microsoft Word and Excel 2007/2010 files larger than 1 MB
- Significant improvement in text extraction time over previous text extraction methods
- Existed in v7.6.3 as well but was disabled by default
  - This means that this feature was already tested in production by some customers already with positive results

LDAP attributes improvements

- Ability to create LDAP query-based groups (populated during user directory import)



Advanced Persistent Threat

- A new threat protection feature was added to the Websense Data Security product
- The feature is based on a set of pre defined policies, ready to use in the Web DLP policies
- The feature is also available for use in WSG, this is built in the product and does not require DSS in addition

Best Practices

Installation and Configuration

TRITON™

- Web security
- Email security
- Data security
- Mobile security

Installation and Configuration

- Avoid using the TRITON management server for running crawler tasks and being an endpoint server
- Use an off-box SQL server to reduce load on the management server
- Make sure Antivirus, Firewall and other security applications are configured to exclude TRITON files and processes
- Use the same user every time the installation package is run

In the event of a problem during installation:

- Copy installation logs to safe location for future technical review
  - Install logs are located in %temp%
  - This temp folder is deleted during restart.
  - Installation logs may help troubleshooting problems that arise later in the process.

Best Practices

Policy Configuration

TRITON™

- Web security
- Email security
- Data security
- Mobile security

Policies configuration

- Optimize the policies used for best performance and reasonable incident in-flow
  - Select policies by region
  - Reduce a policy's number of incidents by:
    - Fine-tuning thresholds
    - Filtering by channel, source or destination
    - Adding exceptions for rules
    - Using cumulative DLP
- Prefer predefined policy templates over custom-defined policies
  - Predefined policies use spheres and pipes which cannot be configured in user defined rules and policies.
- Prefer dictionaries over numerous key phrases
- Malicious Concealment policies may cause false positives and hamper performance and should be used with caution in production mode

Best Practices

Fingerprinting

TRITON™

- Web security
- Email security
- Data security
- Mobile security

Unstructured fingerprints

websense

- Maximum file system size tested:
  - 15 TB
- Every X hashes increase processing time by Y
  - Too many hashes can cause processing time to exceed timeout thresholds
- For optimal accuracy, there should be at least one paragraph of text in files to be fingerprinted
- Consider using machine learning
  - Especially good for documents of same type. For example, contracts, financial statements, source code
  - Machine Learning tasks provide an accuracy percentage. Use it to decide if the Machine Learning classifier should be used
- When using OCR, a different layout from the original document may cause a false negative

Structured fingerprints

- Maximum number of records tested:
  - Network channels – 12M records
  - Endpoint channels – 12M records (5 columns)
- On endpoint channels, use more than one column in the rule and increase the threshold for better accuracy
  - Database fingerprinting classifiers with one row can support about 250 KB entries. Above that, the risk for false positives increases
- When a database is very large (more than 1 MB), consider using predefined policies instead of fingerprints for standard data (SSN's, CCN's names, etc.)
- When fingerprinting people's names, fingerprint first and last name as one column to avoid false positives
- Some field types are not supported:
  - BLOBs (binary large objects)
  - Dates
  - Database proprietary fields

Best Practices

Data Endpoint Agent

TRITON™

- Web security
- Email security
- Data security
- Mobile security

Data Endpoints

- Avoid using the TRITON management server as an endpoint server
- Each endpoint server supports around 15 KB endpoint clients
- Endpoint update check intervals affect the number of endpoints a server can handle
- For load balancing, 2 or more servers should be configured as primary
  - Secondary servers are only accessed when all primary servers fail
- Avoid using file access and process monitoring rules
  - File access and process monitoring have a considerable impact on the machine's overall performance
  - Use these rules judiciously and apply selectively for applications that use channels that are not otherwise monitored for data leakage

Webinar Announcement

websense

Upcoming Webinar

Title: **Upgrading a V-Series appliance to version 7.7**

Date: **October 24, 2012**

Time: **8:30 A.M. PDT (GMT -8)**

How to register:
http://www.websense.com/content/SupportWebinars.aspx

Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit: http://www.websense.com/findaclass
- Websense Training Partners offer classes online and onsite at your location.
- For more information, please send email to: readiness@websense.com

Questions