CA User Activity Reporting Module

Release Notes

Release 12.6

CA Technologies Product References

This document references the following CA Technologies products:

- CA ControlMinder
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA User Activity Reporting Module
- CA IdentityMinder
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- New and Changed Features in r12.6—This chapter describes the provision of the DBExport utility, the addition of two new parameters to Global Configuration and the View Events option, and the option to stop a scheduled job. It also describes the changes to the LMDiag.sh utility.
- Known Issues—The following known issues are added:
  - The Disable Non-CEG Event Data Option Fails on Agents
  - Events Export to PostgreSQL Fails with Fatal Error
- Fixed Issues

Contents

Chapter 1: Welcome

Welcome to CA User Activity Reporting Module. This document contains information about operating system support, enhancements, known issues, and information about contacting CA Technical Support.

Upgrading to CA User Activity Reporting Module Version 12.5 through Subscription

To upgrade CA User Activity Reporting Module to version r12.5, first upgrade to version r12.5 of the Log Manager product, then update all other CA User Activity Reporting Module modules, such as Content, Integration and Agent modules. You perform all upgrade tasks through Subscription.

Important! Upgrade the management CA User Activity Reporting Module server before you install any new CA User Activity Reporting Module servers in your network. Doing so allows the new servers to register properly.

To upgrade to CA User Activity Reporting Module version r12.5

1. Upgrade to Log Manager version r12.5.
   a. Click the Administration tab, Services subtab, expand Subscription Module, and select your CA User Activity Reporting Module management server. By default, this server is the first you installed in your CA User Activity Reporting Module environment.
   b. Click the global/local button to switch to local service configuration.
   c. In the RSS feed URL field, type:

      http://securityupdates.ca.com/CA-ELM/r12.5/RSSFeed_PreUpgrade.xml
   d. In the Modules to Download list, use the arrows to move the Log Manager module from Available to Selected.
   e. Verify that all other required values are configured for the selected server.
   f. Click Update Now.

      When the update is complete, a self-monitoring event appears, indicating that the Log Manager update has been installed. iGateway automatically restarts and your CA User Activity Reporting Module Log Manager session closes. The iGateway restart takes approximately 5 minutes.
   g. Log in to CA User Activity Reporting Module. In the upper right corner of the Log Manager browser window, click About and confirm that the version number indicates the new version of CA User Activity Reporting Module.

      Note: The upgraded CA User Activity Reporting Module r12.5 user interface lists both Subscription Module and Subscription Service under the Administration tab, Services subtab. Subscription Module reflects the interface and functionality previous to the r12.5 update, and is present to help ensure proper communication between all CA User Activity Reporting Module servers during the upgrade to r12.5. Once you have upgraded the Log Manager product on a given CA User Activity Reporting Module server to version r12.5, use only Subscription Service to perform all further subscriptions tasks and configuration changes.
   h. In a federated environment, repeat this process for all CA User Activity Reporting Module servers in your environment, in the following order:
      - Upgrade all subscription proxies to the new version of Log Manager
      - Upgrade all subscription clients to the new version of Log Manager

2. Update all other CA User Activity Reporting Module modules.

   a. Click the Administration tab, click the Services subtab, expand Subscription Service, and select your CA User Activity Reporting Module management server. By default, this server is the first you installed in your CA User Activity Reporting Module environment.

      Important! After you perform Step 1, the upgraded CA User Activity Reporting Module r12.5 user interface lists both Subscription Module and Subscription Service. Use only Subscription Service, and not Subscription Module, to perform all further subscriptions tasks, including the following steps. Subscription Module is present only to help ensure proper communication between all CA User Activity Reporting Module servers during the upgrade to r12.5; do not use it to perform subscription functions post-upgrade.

   b. Click the Administration tab, and click the global/local button to switch to local service configuration.

   c. In the RSS feed URL field, type:

      http://securityupdates.ca.com/CA-ELM/r12.5/RSSFeed.xml

   d. Click Browse, select all CA User Activity Reporting Module modules, and click OK. CA User Activity Reporting Module modules can include Content, Integration, Operating System and Agent updates.

   e. Verify that all other required values are configured for the selected server.

   f. Click Update Now.

      When update is complete, a self-monitoring event appears, indicating that the selected updates have been installed.

   g. If an Operating System module was among the updates installed, reboot the CA User Activity Reporting Module server.

   h. In a federated environment, repeat this process for all CA User Activity Reporting Module servers in your environment, in the following order:

      - Update all subscription proxies with all current CA User Activity Reporting Module modules
      - Update all subscription clients with all current CA User Activity Reporting Module modules

3. If Agent or Connector modules were among the updates, install updated agents and connectors.

   a. Click the Administration tab, click the Log Collection subtab, and select Agent Explorer.

   b. Determine whether to apply subscription updates at the agent explorer level, the agent group level, or the agent level. Select the desired level and click the Subscription button.

   c. Apply updates to agents.

   d. Click the Subscription button again.

   e. Apply updates to connectors.

   Note: For detailed instructions on installing Agents and Connectors, see the *CA User Activity Reporting Module Administration Guide.*

4. Reregister third-party and other CA Technologies products, like CA Access Control, that display CA User Activity Reporting Module reports in their native interfaces using the Open API calls.

   Completing this step updates the certificates that changed in this release. See the *CA User Activity Reporting Module API Programming Guide* for more information.

Note: Review the Release Notes for any Known Issues related to subscription upgrades. If you are upgrading from a release earlier than 12.5, you may experience issues requiring a manual installation of the pre-12.5 upgrade package.

Upgrading to CA User Activity Reporting Module Version 12.5 through Offline Subscription

To upgrade CA User Activity Reporting Module to version r12.5 using offline subscription, you must first download the offline upgrade file package from the CA Technologies FTP site and manually copy it to all offline proxies. You can then upgrade all servers to version r12.5 of the Log Manager product. You must then repeat this process to update all other CA User Activity Reporting Module modules, such as Content, Integration and Agent modules as well.

Note: The following instructions assume that your entire CA User Activity Reporting Module environment is offline, rather than a mixed environment where some servers are online while others are offline. While it is possible to implement a mixed subscription architecture, it is considered best practice to design either an entirely online or entirely offline subscription architecture.

Important! Upgrade the management server before you upgrade or install any new CA User Activity Reporting Module servers in your network. Doing so allows the servers to register properly.

The process to upgrade to CA User Activity Reporting Module Version 12.5 through offline subscription is as follows. For details on each step, see the procedures references in the More Information section.

1. Download and install the pre-12.5 offline upgrade file package from the CA Technologies FTP site.
2. Upgrade all subscription proxies to Log Manager version r12.5.
3. Upgrade all subscription clients to Log Manager version r12.5.
4. Download and install the 12.5 offline upgrade file package from the CA Technologies FTP site.
5. Update all proxies with all other CA User Activity Reporting Module version r12.5 modules.
6. Update all clients with all other CA User Activity Reporting Module version r12.5 modules.
7. If Agent or Connector modules were among the updates, install updated agents and connectors.

After completing the upgrade process, reregister third-party and other CA Technologies products, like CA Access Control, that display CA User Activity Reporting Module reports in their native interfaces using the Open API calls. Completing this step updates the certificates that changed in this release. See the *CA User Activity Reporting Module API Programming Guide* for more information.

Note: Review the *Release Notes* for any Known Issues related to subscription upgrades. If you are upgrading from a release earlier than 12.5., you may experience issues requiring a manual installation of the pre-12.5 upgrade package.

Upgrade Log Manager Application on All Proxies and Clients

Upgrade subscription proxies, then subscription clients to CA User Activity Reporting Module r12.5.

To upgrade subscription proxies and clients to r12.5

1. Upgrade all subscription proxies to Log Manager version r12.5.
   a. Log in to a system in your CA User Activity Reporting Module environment.
   b. Click the Administration tab, Services subtab, expand Subscription Module, and select your CA User Activity Reporting Module management server. By default, this is the first server you installed in your CA User Activity Reporting Module environment.
   c. In the Modules to Download list, use the arrows to move the Log Manager module from Available to Selected. Remove any other modules from the Selected list.
   d. If Offline Subscription Proxy is cleared, select it.
   e. Verify that all other required values are configured for the selected server.
   f. Click Save.
   g. Click Update Now.

      When update is complete, a self-monitoring event appears, indicating that the Log Manager update has been installed. iGateway automatically restarts and your CA User Activity Reporting Module Log Manager session closes.
   h. Log in to CA User Activity Reporting Module. In the upper right corner of the Log Manager browser window, click About and confirm that the version number indicates the new version of CA User Activity Reporting Module.

      Note: The upgraded CA User Activity Reporting Module r12.5 user interface lists both Subscription Module and Subscription Service under the Administration tab, Services subtab. Subscription Module reflects the interface and functionality previous to the r12.5 update, and is present to help ensure proper communication between all CA User Activity Reporting Module servers during the upgrade to r12.5. Once you have upgraded the Log Manager product on a given CA User Activity Reporting Module server to version r12.5, use only Subscription Service to perform all further subscriptions tasks and configuration changes.
   i. In an environment with multiple subscription proxies, copy the offline update .tar file to each proxy in your environment, untar the file according to the instructions in the Download and Install the Pre-12.5 Offline Upgrade Package topic, and repeat this process for all proxies.
2. Upgrade all subscription clients to Log Manager version r12.5.
   a. Click the Administration tab, Services subtab, expand Subscription Module, and select a subscription client.

Note: Offline subscription clients automatically receive all modules that are manually installed on their offline proxy. The contents of the proxy server control which updates the subscription client receives. Modules selected at the local level for an offline client have no effect.

b. Verify that all other required values are configured for the selected server. If you change any settings, click Save.

c. Click Update Now.

When update is complete, a self-monitoring event appears, indicating that the Log Manager update has been installed.

d. Repeat this process for all clients in your environment.

Note: Instead of manually updating each client, you can also set a global subscription schedule to begin an update after confirming that all proxies have been upgraded to version r12.5.

Download and Install the Pre-12.5 Offline Upgrade Package

Begin the upgrade by downloading and installing the pre-12.5 offline file package.

To download and install the pre-12.5 offline upgrade file package from the CA Technologies FTP site

1. On a system with Internet or FTP access, navigate to the FTP offline subscription site:

   ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription

   The directory index displays a folder for each CA User Activity Reporting Module release.
2. Select the 12.5.xx_Offline_Subscription folder, and the Pre_12.5_Upgrade folder.
3. Download the pre-12.5 offline subscription update package. The file name follows the following format:

   subscription_12_5_xx_yy.tar
4. Using physical media such as a disk, or using scp, manually copy the .tar file to the following path on your offline proxy:

   /opt/CA/LogManager/data
5. Log into the default subscription proxy through ssh as the caelmadmin user.
6. Switch to root.
7. Navigate to the following path:

   /opt/CA/LogManager/data
8. Stop iGateway.
9. Rename the existing subscription directory under /data to subscription.bak. For example, rename it to mydir/data/subscription.bak.
10. Untar the tar file using the following command:

    ```
    tar -xvf subscription_12_<x_x_x>.tar
    ```

    This creates a subscription folder and extracts the 12.5 upgrade modules. Correct ownership and permissions are automatically set.
11. Restart iGateway.

Download and Install the 12.5 Offline Upgrade Package

After upgrading all proxies and clients to Log Manager version 12.5, download and install the 12.5 offline upgrade file package from the CA Technologies FTP site.

To download and install the 12.5 offline upgrade file package

1. On a system with Internet or FTP access, navigate to the FTP offline subscription site:

   ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription

   The directory index displays a folder for each CA User Activity Reporting Module release.

2. Select the 12.5.xx_Offline_Subscription folder.
3. Download the offline subscription update package. The file name follows the following format:

   subscription_postupgrade_12_5_xx_yy.zip

4. Using physical media such as a disk, or using scp, manually copy the .zip file to the following file path on your offline proxy:

   /opt/CA/LogManager/data/subscription/offline

Update Proxies and Clients With CA User Activity Reporting Module Modules

After upgrading all servers to Log Manager version 12.5, and installing the 12.5 offline upgrade file package, update subscription proxies, and then subscription clients with all additional CA User Activity Reporting Module modules.

To update proxies and clients with all additional modules

1. Update all proxies with all other CA User Activity Reporting Module version r12.5 modules.
   a. Log in to a system in your CA User Activity Reporting Module environment.
   b. Click the Administration tab, Services subtab, expand Subscription Service and select your CA User Activity Reporting Module management server.

      The Subscription Service Configuration for the selected CA User Activity Reporting Module server appears.

   c. Click the Administration tab.
   d. In the File drop-down, select the offline update .zip file you copied to the server, and click Browse.

      The Modules Available for Download dialog appears.

e. Select the modules you want to download. Modules can include Content, Integration, Operating System and Agent updates.

f. Click Save.

g. Click Update Now.

When update is complete, a self-monitoring event appears, indicating that the selected updates have been installed.

h. In an environment with multiple subscription proxies, copy the offline update .zip file to each proxy in your environment, and repeat this process for all proxies.

2. Update all clients with all other CA User Activity Reporting Module version r12.5 modules.

a. Click the Administration tab, Services subtab, expand Subscription Module, and select a subscription client.

Note: Offline subscription clients automatically receive all modules that are manually installed on their offline proxy. The contents of the proxy server control which updates the subscription client receives. Modules selected at the local level for an offline client have no effect.

b. Verify that all other required values are configured for the selected server. If you change any settings, click Save.

c. Click Update Now.

d. When update is complete, a self-monitoring event appears, indicating that all updates have been installed.

e. Repeat this process for all clients in your environment.

Note: Instead of manually updating each client, you can also set a global subscription schedule to begin an update after confirming that all proxies have been updated with the selected r12.5 modules.

Install Updated Agents and Connectors

If Agent or Connector modules were among the 12.5 update modules, install updated agents and connectors.

To install updated agents and connectors

1. Click the Administration tab, click the Log Collection subtab, and select Agent Explorer.
2. Determine whether to apply subscription updates at the agent explorer level, the agent group level, or the agent level. Select the desired level and click the Subscription button.
3. Apply updates to agents.
4. Click the Subscription button again.
5. Apply updates to connectors.

   Note: For detailed instructions on installing Agents and Connectors, see the *CA User Activity Reporting Module Administration Guide*.

Chapter 2: Operating Environment

This section contains the following topics:

Hardware and Software Environments

CA User Activity Reporting Module installs the CentOS operating system as part of its initial setup. Earlier versions use the Red Hat Enterprise Linux operating system. See the certification matrix for more information.

The CA User Activity Reporting Module Certification Matrix Index lists the links for all CA User Activity Reporting Module certification matrices, including the following:

- Server hardware and software

  CA User Activity Reporting Module Server Hardware and Software Certification Matrix

- Agent hardware and software

  CA User Activity Reporting Module Agent Hardware and Software Certification Matrix

- Log sensors and related operating system support

  CA User Activity Reporting Module LogSensor Certification Matrix

- Product integrations

  CA User Activity Reporting Module Product Integration Matrix

- Certifications with CA Audit iRecorders

  CA User Activity Reporting Module Audit iRecorder Certification Matrix

You can access CA User Activity Reporting Module with the following browsers and the Adobe Flash 9 or 10 player:

- Internet Explorer 9 (FIPS or Non-FIPS modes)
- Mozilla Firefox 16 (FIPS and Non-FIPS modes)

Power Setting Prerequisites for Certain HP and IBM Computers

When CA User Activity Reporting Module is installed on HP Proliant DL 380G5 Series servers and IBM X3650 Series servers with default power use settings, iGateway issues may occur, resulting in slow operation, or other interface issues that may require a manual service restart.

To prevent this potential issue, change the settings before you install CA User Activity Reporting Module.

Note: If you have already installed CA User Activity Reporting Module, you can stop the computer, change the settings as outlined, and restart the computer.

To change the power use settings on HP Proliant DL 380G5

1. Access the BIOS Settings menu.
2. Navigate to the power use settings.
3. Select “OS Control Mode” from the available choices.

   Note: The default setting is “HP Dynamic Power Settings Mode”.

To change the power use settings on IBM X3650

1. Access the BIOS Settings menu.
2. Navigate to the power use settings.
3. Disable the following parameters:
   - Active Energy Manager
   - Enhanced C1 Power State

Monitor Resolution

The minimum requirement for monitor resolution is 1024 x 768 pixels. For best viewing, a monitor resolution of 1280 x 1024 is recommended.

CA EEM Server References

For information about operating system support for an existing CA EEM server, see the *CA Embedded Entitlements Manager Getting Started* guide. This guide is included on the CA User Activity Reporting Module bookshelf.

You can also download this bookshelf from Technical Support. For assistance, contact CA Support at http://ca.com/support.

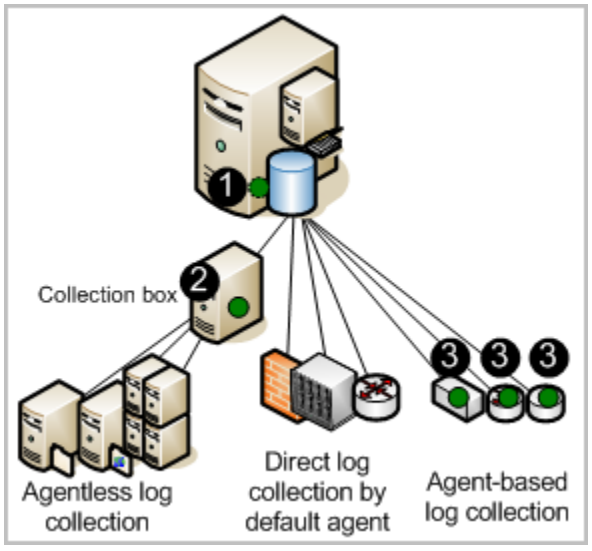
Chapter 3: Features

This section contains the following topics:

Log Collection

The CA User Activity Reporting Module server can be set up to collect logs using one or more supported techniques. The techniques differ in the type and location of the component that listens for and collects the logs. These components are configured on agents.

The following illustration depicts a single-server system, where agent locations are indicated with a dark (green) circle.



The numbers on the illustration refer to these steps:

1. Configure the default agent on the CA User Activity Reporting Module to fetch events directly from the syslog sources you specify.
2. Configure the agent installed on a Windows collection point to collect events from the Windows servers you specify and transmit them to the CA User Activity Reporting Module.
3. Configure agents installed on hosts where event sources are running to collect the configured type of events and perform suppression.

Note: Traffic from the agent to the destination CA User Activity Reporting Module server is always encrypted.

Consider the following advantages of each log collection technique:

- Direct log collection

  With direct log collection, you configure the syslog listener on the default agent to receive events from the trusted sources you specify. You can also configure other connectors to collect events from any event source that is compatible with the soft appliance operating environment.

  Advantage: You do not need to install an agent to collect logs from event sources that are in close network proximity to the CA User Activity Reporting Module server.

- Agentless collection

  With agentless collection, there is no local agent on the event sources. Rather, an agent is installed on a dedicated collection point. Connectors for each target event source are configured on that agent.

  Advantage: You can collect logs from event sources running on servers where you cannot install agents, such as severs where corporate policy prohibits agents. Delivery is guaranteed, for example, when ODBC log collection is configured properly.

- Agent-based collection

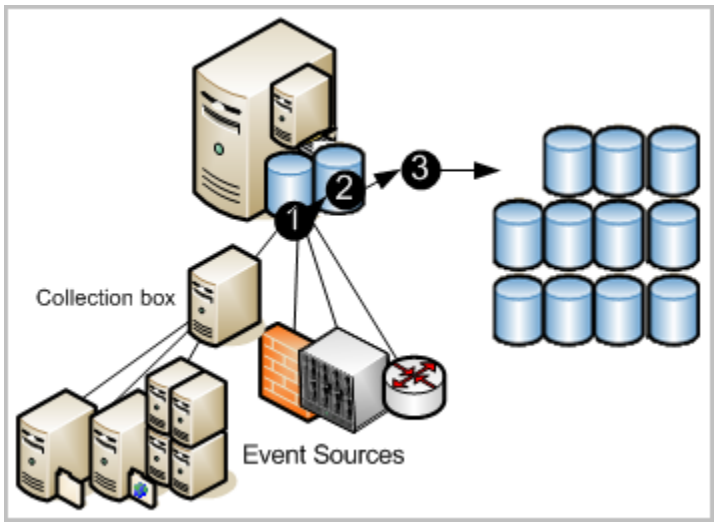
  With agent-based collection, an agent is installed where one or more event sources are running and a connector is configured for each event source.

  Advantage: You can gather logs from a source where the network bandwidth between that source and the CA User Activity Reporting Module is not good enough to support direct log collection. You can use the agent to filter the events and reduce the traffic sent across the network. Event delivery is guaranteed.

Note: See the *Administration Guide* for details on agent configuration.

Log Storage

CA User Activity Reporting Module provides managed embedded log storage for recently archived databases. Events collected by agents from event sources go through a storage lifecycle as illustrated by the following diagram.



The numbers on the illustration refer to these steps:

1. New events collected by any technique are sent to the CA User Activity Reporting Module. The state of incoming events depends on the technique used to collect them. Incoming events must be refined before being inserted into the database.
2. When the database of refined records reaches the configured size, all records are compressed into a database and saved with a unique name. Compressing log data reduces the cost of moving it and reduces the cost of storage. The compressed database can either be moved automatically based on auto-archive configuration or you can back it up and move it manually before it reaches the age configured for deletion. (Auto-archived databases are deleted from the source as soon as they are moved.)
3. If you configure auto-archive to move the compressed databases to a remote server on a daily basis, you can move these backup to off-site long-term log storage at your convenience. Retaining backups of logs enables you to comply with the regulations that state that logs must be securely collected, centrally stored for a certain number of years, and available for review. (You can restore database from long-term storage at any time.)

Note: See the *Implementation Guide* for details on configuring the event log store, including how to set up auto-archiving. See the *Administration Guide* for details on restoring the backups for investigation and reporting.

Standardized Presentation of Logs

Logs generated by applications, operating systems, and devices all use their own formats. CA User Activity Reporting Module refines the collected logs to standardize the way the data is reported. The standard format makes it easier for auditors and upper management to compare data collected from different sources. Technically, the CA Common Event Grammar (CEG) helps implement event normalization and classification.

The CEG provides several fields which are used to normalize various aspects of the event, including the following:

- Ideal Model (Class of technologies such as antivirus, DBMS, and firewall)
- Category (Examples include Identity Management and Network Security)
- Class (Examples include Account Management and Group Management)
- Action (Examples include Account Creation and Group Creation)
- Results (Examples include Success and Failure)

Note: See the *CA User Activity Reporting Module Administration Guide* for details on the rules and files used in event refinement. See the section on Common Event Grammar in the online help for details on the normalizing and categorizing events.

Compliance Reporting

CA User Activity Reporting Module lets you gather and process security-relevant data and turn it into reports suitable for internal or external auditors. You can interact with queries and reports for investigations. You can automate the reporting process by scheduling report jobs.

The system provides:

- Easy to use query capability with tags
- Near-real time reporting
- Centrally searchable, distributed archives of critical logs

Its focus is on compliance reporting rather than real-time correlation of events and alerts. Regulations demand reporting that demonstrates compliance with industry-related controls. CA User Activity Reporting Module provides reports with the following tags for easy identification:

- Basel II
- COBIT
- COSO
- EU Directive - Data Protection
- FISMA
- GLBA
- HIPAA
- ISO\IEC 27001\2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS 70
- SOX

You can review predefined log reports or perform searches based on criteria you specify. New reports are provided with subscription updates.

Log view capabilities are supported by the following:

- On demand query capability with predefined or user-defined queries, where results can include up to 5000 records

- Quick search, through Prompts, for a specified host name, IP address, port number, or user name
- Scheduled and on demand reporting with out-of-the-box reporting content
- Scheduled query and alerting
- Basic reports with trending information
- Interactive, graphical event viewers
- Automated reporting with email attachment
- Automated report retention policies

Note: For details on using predefined queries and reports or creating your own, see the *CA User Activity Reporting Module Administration Guide*.

Policy Violation Alerting

CA User Activity Reporting Module lets you automate the sending of an alert when an event occurs that requires near-term attention. You can also monitor action alerts from CA User Activity Reporting Module at any time by specifying a time interval, such as from the last five minutes to the last 30 days. Alerts are automatically sent to an RSS feed that can be accessed from a web browser. Optionally, you can specify other destinations, including email addresses, a CA IT PAM process such as one that generates help desk tickets, and one or more SNMP trap destination IP addresses.

To help you get started, many predefined queries are available for scheduling as action alerts, as is. Examples include:

- Excessive user activity
- High CPU utilization average
- Low available disk space
- Security event log cleared in last 24 hours
- Windows audit policy changed in last 24 hours

Some queries use keyed lists, where you supply the values used in the query. Some keyed lists include predefined values that you can supplement. Examples include default accounts and privileged groups. Other keyed lists, such as that for business critical resources, have no default values. After you configure them, alerts can be scheduled for predefined queries such as:

- Group membership addition or removal by privileged groups
- Successful login by default account
- No events received by business critical sources

Keyed lists can be updated manually, by importing a file, or by running a CA IT PAM dynamic values process.

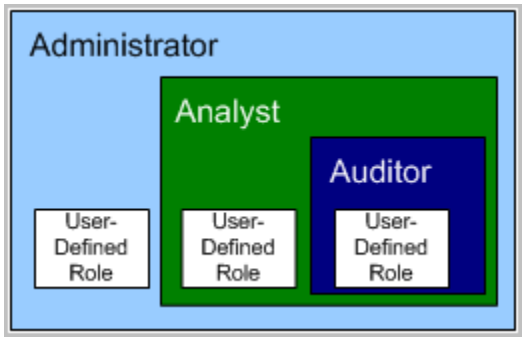
Note: See the *CA User Activity Reporting Module Administration Guide* for details on action alerts.

Role-Based Access

CA User Activity Reporting Module provides three predefined application groups or roles. Administrators assign the following roles to users to specify their access rights to CA User Activity Reporting Module features:

- Administrator
- Analyst
- Auditor

The Auditor has access to few features. The Analyst has access to all Auditor features plus more. The Administrator has access to all features. You can define a custom role with associated policies that limit user access to resources in the way that suits your business needs.



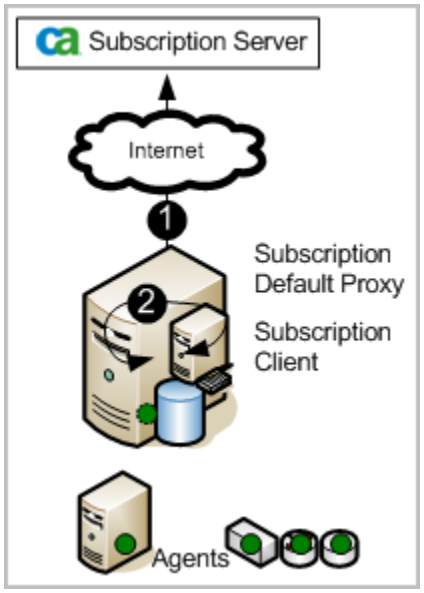
Administrators can customize access to any resource by creating a custom application group with associated policies and assigning that application group, or role, to user accounts.

Note: See the *CA User Activity Reporting Module Administration Guide* for details on planning and creating custom roles, custom policies, and access filters.

Subscription Management

The subscription module is the service that enables subscription updates from the CA Technologies Subscription Server to be automatically downloaded on a scheduled basis and distributed to CA User Activity Reporting Module servers. When a subscription update includes the module for agents, users initiate the deployment of these updates to agents. *Subscription update*s are updates to CA User Activity Reporting Module software components and operating system updates, patches, and content updates such as reports.

The following illustration depicts the simplest direct Internet connection scenario:



The numbers on the illustration refer to these steps:

1. The CA User Activity Reporting Module server, as the default subscription server, contacts the CA Subscription server for updates and downloads any new available updates. The CA User Activity Reporting Module server creates a backup, then pushes content updates to the embedded component of the management server that stores content updates for all other CA User Activity Reporting Modules.
2. The CA User Activity Reporting Module server, as a subscription client, self-installs the product and operating system updates it needs.

Note: See the *Implementation Guide* for details on planning and configuring subscription. See the *Administration Guide* for details on refining and modifying the subscription configuration and for applying updates to agents.

Support for IPv6 IP Addresses

Previously, specification of IP Addresses was limited to IPv4 dotted decimal notation. With the current release, you can now specify IPv6 addresses in any IP Address field. IPv6 uses 128-bit IP addresses instead of the 32-bit addresses used by IPv4. Any policies that are based on the IP address version support IPv6 and IPv4.

You can use IPv4-mapped IPv6 addresses or the traditional IPv6 format. The IPv4-mapped IPv6 address format allows the IPv4 address of an IPv4 node to be represented as an IPv6 address as follows:

- The preferred IPv6 form is written as eight groups of four hexadecimal digits (x:x:x:x:x:x:x:x). Each x is one to four hexadecimal digits of the eight 16-bit pieces of the address.
- The IPv4-mapped IPv6 address, convenient in a mixed environment of IPv4 and IPv6 nodes is 0:0:0:0:0:FFFF:d.d.d.d, where each d is a decimal value of the address (IPv4 dotted decimal notation).

  Important! IPv4-compatible IPv6 addresses in the format 0:0:0:0:0:0:d.d.d.d are now deprecated, according to RFC 4291, because the current IPv6 transition mechanisms no longer use these addresses.

The following is a valid IPv6 address written in traditional format.

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

If one or more four-digit groups are 0000, the zeros can be omitted and replaced with two colons(::). Leading zeros in a group can also be omitted. The following example IP addresses are equivalent:

- 2001:0db8:0000:0000:0000:0000:1428:57ab
- 2001:0db8::1428:57ab
- 2001:db8:0:0:0:0:1428:57ab
- 2001:db8::1428:57ab

If you are replacing IPv4 addresses with IPv4-mapped addresses, use the following examples as guidelines:

- 0:0:0:0:0:FFFF:192.168.2.128
- 0:0:0:0:0:FFFF:172.16.2.128

Alternatively, you can use the following compressed form:

- ::FFFF:192.168.2.128
- ::FFFF:172.16.2.128

Chapter 4: New and Changed Features in r12.6

This section contains the following topics:

Export Archived Databases into an RDBMS

The DBExport Service feature lets you export the archived databases from the CA User Activity Reporting Module server into an RDBMS such as Microsoft SQL, Oracle, or PostgreSQL in your environment.

For information about exporting the archived databases, see the Export the Archived Databases into RDBMS scenario.

View Events upto 5000 in a Dialog

You can click View Events in query viewer to view events upto 5000 in a dialog. You can search or sort events in that dialog.

For information about View Events, see the *Online Help*.

Stop Scheduled Report Job

You can stop a scheduled report job if it takes a longer time to run.

For information about these parameters, see the *CA User Activity Reporting Module Administration Guide* or *Online Help*.

New Parameters in Global Configuration

The Global Configuration page contains the following parameters:

- Disable Non-CEG Event Data
- Process the CDATA Delimiter in Query Result

For information about these parameters, see the *CA User Activity Reporting Module Implementation Guide* or *Online Help*.

Enhancements to the LMDiag.sh Utility

The LMDiag.sh utility is enhanced to generate an improved diagnostic file.

Support for Hyper-V Server 2012

You can install CA User Activity Reporting Module ISO on Hyper-V Server 2012. After the installation, you must install LinuxIC v3.4 for Hyper-V to enable synthetic device support. For downloading LinuxIC v3.4, see www.microsoft.com www.microsoft.com.

Chapter 5: New and Changed Features in r12.5.07

This section contains the following topics:

Upgraded Support for Tomcat 7.0.40

Tomcat has been upgraded to 7.0.40 to resolve vulnerabilities.

Utility to Change the Hostname and IP Address of a Server

The Rename_elm.sh utility is modified to change the hostname and IP address of a CA User Activity Reporting Module server in your standalone or federation environment.

For information about using the utility to change the hostname and IP address of a server, see the *Scenarios*.

Chapter 6: New and Changed Features in r12.5.06

This section contains the following topics:

Support for an Agent on Windows 2012, Windows 8, RHEL 6 x64-bit, and SUSE 11 x64-bit Platforms

You can deploy a CA User Activity Reporting Module agent on Windows 2012, Windows 8, RHEL 6 x64-bit, and SUSE 11 x64-bit platforms.

Upgraded Support for CA iTechnology iGateway

CA iTechnology iGateway has been upgraded to 4.6.1.19 to resolve the vulnerability in redirecting URL in the base spindle.

Distribution of the Partprobe Utility

The Operation System packages have been enhanced to deliver the Partprobe utility.

Chapter 7: New and Changed Features in r12.5.05

This section contains the following topics:

Support Dropped for RHEL 4 and VMware ESX 3.5 Agents

CA User Activity Reporting Module dropped its support for RHEL4 and VMware ESX 3.5 agents from this release.

Support for an Agent on RHEL 6 32-bit Platforms

You can deploy a CA User Activity Reporting Module agent on RHEL 6 32-bit platforms.

Support for the CSV Format in Reports and Schedule Reports

You can export reports and scheduled reports in the CSV format too.

Support for Enabling or Disabling the CA Adapters Services

You can enable or disable the CA Adapters services based on your usage of CA Adapters.

For information about enabling or disabling the CA Adapters services, see the *CA User Activity Reporting Module Administration Guide 12.5.05*.

Updated Version Support for CA EEM, Tomcat, and CENTOS

CA User Activity Reporting Module is updated to support CA EEM Release 8.4.SP4 CR14, Tomcat 7.0.30, and CENTOS 5.8.

Updated Support for Internet Explorer 9 and Mozilla Firefox 16

CA User Activity Reporting Module supports Internet Explorer 9 and Mozilla Firefox 16 too.

Chapter 8: New and Changed Features in r12.5.04

This section contains the following topics:

Updated CA ControlMinder for Virtual Environments Integrations

CA User Activity Reporting Module is updated to enhance the performance of the CA ControlMinder for Virtual Environments integrations, deployment of connectors through webservices, and the performance of CA User Activity Reporting Module. The following changes are made in CA User Activity Reporting Module:

- UARM displays the error code 507 if the agent is in the configuration pending state when you deploy a connector through webservices.
- The OOTB EEM policies include the scoping policies that are required for CA ControlMinder for Virtual Environments.
- You can use the same certificate for all openAPI and Webservices API authentications.

Updated Support for CA EEM

CA User Activity Reporting Module is updated to support CA EEM Release 8.4 SP4 CR13.

Chapter 9: New and Changed Features in r12.5.03

This section contains the following topics:

Catalog Database Partitioning

By default, CA User Activity Reporting Module now partitions the catalog database. The feature verifies that the catalog database does not grow indefinitely in size, and reduces the disk space.

Agent Support on RHEL 5 x64-bit Systems

You can install the CA User Activity Reporting Module agent on a RHEL 5 x64-bit system.

Information about installing the agent is available in the *CA User Activity Reporting Module Agent Installation Guide*.

CPU Throttling

You can throttle the CPU usage of a connector. The CA User Activity Reporting Module logsensor receives events according to the allocated CPU usage.

For information about CPU throttling, see the *CA User Activity Reporting Module Administration Guide*.

CA User Activity Reporting Module High Availability

You can enable CA User Activity Reporting Module High Availability in your virtual environment through VMware High Availability (VMware HA). CA User Activity Reporting Module supports the VMware HA features without any configuration.

For information about the CA User Activity Reporting Module High Availability, see the *CA User Activity Reporting Module Implementation Guide*.

CA User Activity Reporting Module as a Virtual Appliance

The updated CA User Activity Reporting Module as a Virtual Appliance feature does not require manual setting of the paravirtualization settings in the provisioned CA User Activity Reporting Module server.

Information about deploying CA User Activity Reporting Module as a virtual appliance is available in the *CA User Activity Reporting Module Implementation Guide.*

Chapter 10: New and Changed Features in r12.5.02

This section contains the following topics:

Product Name Change

CA Enterprise Log Manager has been renamed CA User Activity Reporting Module. All features and functionality introduced in CA Enterprise Log Manager versions up to 12.5.01 are still included.

More information:

Screen Captures May Show CA User Activity Reporting Module Title (see page 99)

Data Integrity Checking on Raw Events

You can check raw event data for tampering. CA User Activity Reporting Module uses digital signatures to validate the event data. If the database is corrupted or if its signature is missing or corrupted, the data integrity check considers the data tampered.

You can schedule integrity checks to occur at set times and on selected CA User Activity Reporting Module servers, or on demand. This functionality is an extension of the existing data integrity checking feature that only applied to archived event data.

For more information about Data Integrity Checking, see the *CA User Activity Reporting Module Online Help.*

External ODBC Database Connection

You can directly query an external ODBC database. This feature allows you to target CA User Activity Reporting Module reports and queries to ODBC databases in addition to the internal event log store.

You must configure a connection to each ODBC database you want to target. For more information on ODBC database connections, see the *CA User Activity Reporting Module Online Help*.

Virtual Automation API

You can deploy event collection for virtual machines using the Virtual Automation API for CA User Activity Reporting Module. You can use the API to trigger a preset collection profile, which contains all the information necessary to provision event collection.

For more information, see the *CA User Activity Reporting Module Virtual Automation API Guide.*

Chapter 11: New and Changed Features in r12.5.01

This section contains the following topics:

Integration with ObserveIT

You can integrate CA User Activity Reporting Module with ObserveIT v5.2.50 to investigate user session recordings. CA User Activity Reporting Module provides you the option to monitor configuration activities of a user by viewing user session recordings, and generate reports.

For information about the integration of CA User Activity Reporting Module with ObserveIT, see the *CA User Activity Reporting Module Administration Guide* and *CA User Activity Reporting Module Online Help*.

Keyed Lists

This updated feature enhances the performance of keyed lists. With this feature, you can schedule keyed list updates using IT PAM dynamic value process. The IT PAM dynamic values process periodically updates the specified Users list with the latest values.

Information about the enhanced keyed lists is available in the *CA User Activity Reporting Module Administration Guide* and *Online Help.*

Header and Footer in Reports

The Report Server is updated to include a header and footer in PDFs. You can configure the Report Server to generate a header and footer, and related attributes.

Information about the Report Server is available in the *CA User Activity Reporting Module Administration Guide* and *Online Help.*

Datetime Format

You can use the CA User Activity Reporting Module locale properties files to change the default datetime format to a datetime format of your choice. The configured datetime format is displayed on the UI, query and report results.

Information about the datetime formats is available in the *CA User Activity Reporting Module Administration Guide* and *Online Help.*

View Query

The updated Query Cursor feature enhances the appearance of the query results. The most recent results appear first in the results table. To view additional results, you must click the arrow keys or select a range of rows from the list. If the query results are not grouped, the list displays the row ranges you have viewed, and the next sequential range available. If the query results have been grouped, the list displays all rows ranges available in the entire results set.

Information about queries is available in the *CA User Activity Reporting Module Administration Guide* and *Online Help.*

Replace IP Address of an Event Source with Hostname

This new feature lets the agent to replace the IP address of an event source with the hostname of the event source. All the connectors within the agent inherit this feature. If you want to enable the feature for all the agents in your environment, configure each agent separately.

Information about the updated agent feature is available in the *CA User Activity Reporting Module Administration Guide* and *Online Help.*

Agent Diagnostic File

You can review the log files and configuration files of a selected CA User Activity Reporting Module agent using CA User Activity Reporting Module AgentDiagnostics utility. The utility packages system information and log files into a compressed .tar file for transmission to CA Technologies Support personnel. You can transfer this file using FTP or another file transfer method.

Information about the AgentDiagnostics utility is available in the *CA User Activity Reporting Module Administration Guide* and *Online Help.*

Considerations for CA Access Control Users

The updated Considerations for CA Access Control users contains information about securing CA User Activity Reporting Module using CA Access Control, and an updated reference to the Connector Guide for CA Access Control required to integrate CA User Activity Reporting Module with CA Access Control.

Information about the considerations for CA Access Control users is available in the *CA User Activity Reporting Module* Implementation *Guide*.

CA User Activity Reporting Module as a Virtual Appliance

The updated OVF template contains a new parameter, NTP Server Location.

Information about the updated OVF template is available in the *CA User Activity Reporting Module* Implementation *Guide.*

Agent Support on Microsoft Windows 64-bit Systems

You can install the CA User Activity Reporting Module agent on a Microsoft Windows 64-bit system.

Information about installing the agent is available in the *CA User Activity Reporting Module Agent Installation Guide*.

Chapter 12: New and Changed Features in r12.5

This section contains the following topics:

Event Correlation

You can use event correlation rules to detect complex patterns of events that are associated with unusual or dangerous states, or with suspicious activity. CA User Activity Reporting Module provides numerous predefined correlation rules, and the ability to create custom rules or modify predefined ones.

You could deploy a prefined correlation rule to detect suspicious activity after a specified number of failed logins. For example you could use the "5 Failed Logins by a single account followed by excessive configuration management activity" rule. In this case, you could also customize the number of failed logins, or the definition of excessive activity.

For more information about Event Correlation, see the *CA User Activity Reporting Module Implementation Guide* and *CA User Activity Reporting Module Online Help.*

Incident Management

You can view and respond to incidents generated by CA User Activity Reporting Module event correlation using the Incident Management system. You can investigate the events that make up an incident, routing incident notifications, or triggering automatic workflows.

For example, you can view current incidents in your environment. You could sort them by severity to see the most severe first, and view each in turn checking to see that the assigned severity is appropriate. You can then downgrade incidents not worthy of immediate attention, and assign any incidents to an appropriate resource, or view comments attached to that incident.

For more information about Incident Management, see the *CA User Activity Reporting Module Administration Guide* and *CA User Activity Reporting Module Online Help.*

Compliance Dashboards

Compliance Dashboards let you quickly check the status of your environment with respect to specified states or regulations.

For example, you can open CA User Activity Reporting Module and view the PCI Incidents Dashboard. The dashboard shows you various high-level status displays, including:

- A summary of all PCI-standard related events found in your environment.
- A trending panel tracking PCI events over the recent past.
- A meter showing green/red/yellow overall status based on the number of events.

Data Integrity Checking

You can check archived or recataloged data for tampering, helping to secure your archived data, and meet regulatory requirements. CA User Activity Reporting Module uses digital signatures to validate the databases. If the database is corrupted or if its signature is missing or corrupted, the data integrity check considers the database tampered.

You can schedule daily data integrity checks to occur at set times and on selected CA User Activity Reporting Module servers. Any tampered databases detected by a scheduled integrity check are automatically quarantined. You can view quarantined databases and decide whether to regenerate keys to make them queriable.

For more information about Data Integrity Checking, see the *CA User Activity Reporting Module Online Help.*

Improved Subscription Monitoring

You can view the current subscription status of your global CA User Activity Reporting Module environment through the Subscription Dashboard. The Subscription Dashboard displays the progress of any updates currently being downloaded or installed by any CA User Activity Reporting Module server. For example, during a scheduled update to your global CA User Activity Reporting Module environment, you can use the Subscription Dashboard to monitor the update progress of each CA User Activity Reporting Module server, including which modules are currently downloading or installing, and the current state of the server. From the Subscription Dashboard, you can also see the state of any content updates currently in progress, as well as a list of all content updates previously installed.

You can view the current subscription status of a specific CA User Activity Reporting Module server through the global Subscription Dashboard, or through the server's local State window.

For more information about Improved Subscription Monitoring, see the *Subscription* section of the *CA User Activity Reporting Module Administration Guide*.

Nested Category Tags

You can create custom nested category tags for queries and reports. Nested tags let you organize reports and queries into detailed subcategories.

For example, CA User Activity Reporting Module provides a report category tag named Event Categories. You could add custom tags based on event categories in your environment.

For more information about nested category tags, see the *CA User Activity Reporting Module Online Help*.

CA Access Control PUPM

CA User Activity Reporting Module supports CA Access Control privileged user password management (PUPM). CA Access Control PUPM events include a check-out and check-in time, recording when a password is in use. These times are mapped to event_start_time_gmt and event_end_time_gmt in the updated CEG schema for this release.

You can use advanced drilldown to investigate user activity by choosing the new fields as advanced filters in your queries. For example, you could right-click on a user in a CA Access Control report panel, and apply a filter like the following to the report you drilling down into:

```
(event_time_gmt >= event_start_time_gmt) AND (event_time_gmt <= event_end_time_gmt)
```

This filter displays the check-out and check-in time from the selected user event.

For more information about drilldowns and filtering for CA Access events see the *CA User Activity Reporting Module Online Help*.

Large Query Support

You can set a query to search more than 5,000 event database rows, letting you make broader searches. In previous releases, the maximum number of events a query could return was 5,000.

When creating or editing a query, you can set a higher limit from the Result Conditions step of the query design wizard in either of the following ways:

- Setting the Row Limit value in the results area to a number higher than 5,000.
- Selecting the No Limit button in the results area.

Note: If a scheduled report includes a large query, you cannot publish it to PDF due to a limitation of the format.

For more information about large queries see the *CA User Activity Reporting Module Online Help*.

CA User Activity Reporting Module Sizing Calculator

The current release includes a sizing calculator which can help provide guidance for the number of CA User Activity Reporting Module servers required to meet the needs of your environment. You can input your hardware details, the various types of event sources you want to monitor, how long you must retain event data, and receive a suggested number of CA User Activity Reporting Module servers.

The calculator also includes expected event-per-second rates for all listed event sources. You can accept or adjust these default values.

The installation package includes the sizing calculator, which must be installed on Windows.

Chapter 13: New and Changed Features in r12.1 SP3

The CA User Activity Reporting Module r12.1 SP3 release contains bug fixes of CA User Activity Reporting Module r12.1 SP2.

Chapter 14: New and Changed Features in r12.1 SP2

This section contains the following topics:

CA User Activity Reporting Module as a Virtual Appliance

You can deploy CA User Activity Reporting Module as a virtual appliance in the Open Virtualization Format (OVF). The virtual appliance requires less time to provision than the time required to provision a CA User Activity Reporting Module server on a virtual machine.

OVF is an open standard for packaging and distributing virtual appliances. CA User Activity Reporting Module uses the Virtual Machine Disk (VMDK) file format based on OVF.

Information about deploying CA User Activity Reporting Module as a virtual appliance is available in the *Implementation Guide.*

Simplified Agent Administration

This updated feature simplifies provisioning of a new CA User Activity Reporting Module server. With this feature, you can:

- Update a list of CA User Activity Reporting Module servers at the Agent Explorer level or an individual agent group level.
- Add a new server to an existing server list, and CA User Activity Reporting Module updates the server list in each agent.

Information about this simplified agent administration is available in the *Administration Guide* and *Online Help.*

Role-Based Access Control in API Login Calls

You can perform role-based access control on a user logged on to CA User Activity Reporting Module through API. You can define the data access filters applied to the query, in XML format. You could use this specification to filter a query or report result according to your role when you use the certificate name and password authentication.

Information about the access filter XML is available in the *API Programming Guide.*

LogSensor Help Files

A LogSensor Guide for each logsensor is provided with this release. You can access a LogSensor Guide from the Integration Wizard of the UI.

Retain a Report Configuration

You can retain the configuration of a report by selecting the Retain after Expiry option in the Schedule Report wizard. After the report is generated, you can modify the report configuration and reschedule the report. This feature is valid for both the run-once and run-now reports.

Information about this simplified agent administration is available in the *Administration Guide* and *Online Help.*

Chapter 15: New and Changed Features in r12.1 SP1

This section contains the following topics:

FIPS 140-2 Compliance Overview

The Federal Information Processing Standards (FIPS) 140-2 publication is a security standard for the cryptographic libraries and algorithms a product should use for encryption. FIPS 140-2 encryption affects the communication of all sensitive data between components of CA Technologies products and between CA Technologies products and third-party products. FIPS 140-2 specifies the requirements for using cryptographic algorithms within a security system protecting sensitive, unclassified data.

CA User Activity Reporting Module offers FIPS compatibility with event traffic secured using FIPS-compliant algorithms when operating in FIPS mode. CA User Activity Reporting Module also offers a default, non-FIPS mode in which event traffic is *not* secured with FIPS-compliant algorithms. CA User Activity Reporting Module servers in a federated network cannot mix the two operating modes. This means that a server running in non-FIPS mode cannot share query and report data with a server that is running in FIPS mode.

Information about enabling and disabling FIPS mode is available in the *Implementation Guide* section on installing CA User Activity Reporting Module, and in the online help for the System Status service.

More information:

Operating Modes (see page 68)
Encryption Libraries (see page 69)
Algorithms Used (see page 69)
About Certificates and Key Files (see page 70)
FIPS Support Limitations (see page 71)
Configure Mozilla Firefox to Access CA User Activity Reporting Module in FIPS Mode (see page 73)

Operating Modes

CA User Activity Reporting Module can operate in two modes, FIPS mode or non-FIPS mode. The cryptographic boundaries are the same in both modes, but the algorithms are different. By default, CA User Activity Reporting Module servers operate in non-FIPS mode. Users with the Administrator role can enable FIPS mode operation.

non-FIPS mode

This mode uses a mix of encryption algorithms for event transport and other communications between the CA User Activity Reporting Module and CA EEM server that do not necessarily meet FIPS 140-2 standards.

FIPS mode

This mode uses FIPS-certified encryption algorithms for event transport and other communications between the CA User Activity Reporting Module and CA EEM server.

Administrator-level users can review agent operating modes from the Agent Explorer node on the Administration tab, Log Collection subtab.

For more information about switching between FIPS and non-FIPS modes, refer to the online help for System Status Tasks, or the *Implementation Guide* section on configuring services.

More information:

Algorithms Used (see page 69)
FIPS Support Limitations (see page 71)

Encryption Libraries

The Federal Information Processing Standards (FIPS) 140-2 publication specifies the requirements for using cryptographic algorithms within a security system protecting sensitive, unclassified data.

CA User Activity Reporting Module also embeds the Crypto-C Micro Edition (ME) v2.1.0.2 cryptographic library from RSA, which has been validated as meeting the FIPS 140-2 *Security Requirements for Cryptographic Modules.* The validation certificate number for this module is 865.

Algorithms Used

Computer products that use FIPS 140-2 certified cryptographic modules in FIPS mode can use only FIPS-approved security functions. These include AES (Advanced Encryption Algorithm), SHA-1 (Secure Hash Algorithm), and higher level protocols such as TLS v1.0 as explicitly allowed in the FIPS 140-2 standard and implementation guides.

In non-FIPS mode, CA User Activity Reporting Module uses the following algorithms:

- AES 128
- Triple DES (3DES)
- SHA-1
- MD5
- SSL v3

In FIPS mode, CA User Activity Reporting Module uses the following algorithms:

- AES 128
- Triple DES (3DES)
- SHA-1
- TLS v1

CA User Activity Reporting Module uses SHA-1 as the default digest algorithm to encrypt passwords and sign server requests.

CA User Activity Reporting Module uses TLS v1.0 for communications with external LDAP directories if the LDAP connection uses TLS, communications between iTechnology components, the agent to iGateway service communication in FIPS mode, and the event channel between an agent and the logDepot service.

More information:

FIPS Support Limitations (see page 71)

About Certificates and Key Files

For FIPS 140-2 support, the upgrade to CA User Activity Reporting Module r12.1 SP1 converts existing P12 format certificates to PEM format certificates. This conversion results in the generation of the following files:

- Certificate file with a .cer extension
- Key file with a .key extension

Key files are not encrypted, and it is up to the user to secure them from unauthorized access on both server and agent hosts. The CA User Activity Reporting Module soft-appliance uses various operating system hardening techniques to protect keys and certificates stored in the file system. CA User Activity Reporting Module does not support the use of external key storage devices.

CA User Activity Reporting Module uses the following certificates and key files:

Certificate/Key File Name	Location	Description
CAELMCert	/opt/CA/SharedComponents/iTechnology (You can refer to this directory using the shorter variable name, $IGW_LOC.)	All CA User Activity Reporting Module services use this certificate for communications between CA User Activity Reporting Module servers, and between CA User Activity Reporting Module servers and the CA EEM server. An entry for this certificate, and its corresponding key file, exists in the main configuration file, CALM.cnf. The tag pairs begin <Certificate> and <KeyFile> respectively.
CAELM_AgentCert	$IGW_LOC on the agent host server	Agents use this certificate to communicate with any CA User Activity Reporting Module server. The CA User Activity Reporting Module Management server provides this certificate to the agent. The certificate is valid for any CA User Activity Reporting Module server within a given application instance.

Certificate/Key File Name	Location	Description
itpamcert	IT PAM server	This certificate is used for communications with IT PAM. See the CA IT PAM documentation for additional information.
rootcert	$IGW_LOC	This certificate is a self-signed, root certificate signed by iGateway during installation.
iPozDsa	$IGW_LOC	The CA EEM server, both local and remote, uses this certificate. See the CA EEM documentation for additional information.
iPozRouterDsa	$IGW_LOC	The CA EEM server, both local and remote, uses this certificate. See the CA EEM documentation for additional information.
iTechPoz-trusted	/opt/CA/Directory/dxserver/config/ssld	CA Directory uses this certificate.
iTechPoz-<hostname>-Router	/opt/CA/Directory/dxserver/config/ssld	CA Directory uses this certificate.

FIPS Support Limitations

The following CA User Activity Reporting Module features and product interoperations do not support FIPS mode operations:

ODBC and JDBC Access to the Event Log Store

ODBC and JDBC in CA User Activity Reporting Module relies on an underlying SDK that does not support FIPS mode operations. Administrators of federated networks that require FIPS operations must manually disable the ODBC service on each CA User Activity Reporting Module server. See the section in the *Implementation Guide* about disabling ODBC and JDBC access to the event log store.

Sharing a CA EEM Server

CA User Activity Reporting Module r12.1 SP1 uses CA EEM r8.4 SP3, which is FIPS compatible. Enabling FIPS mode on the CA User Activity Reporting Module server disables the communication between the shared CA EEM and any product that does not support CA EEM r8.4 SP3.

For example, CA IT PAM is not FIPS compatible. If you upgrade your CA User Activity Reporting Module server to FIPS mode, the intergration with CA IT PAM fails.

You can share a CA EEM server between CA User Activity Reporting Module r12.1 SP1 and CA IT PAM r2.1 SP2 and r2.1 SP3 in non-FIPS mode only.

If your CA IT PAM installation is not sharing the same CA EEM server, CA User Activity Reporting Module r12.1 SP1 can run in FIPS mode and it can communicate with CA IT PAM; howvever, those communication channels are not FIPS compatible.

LDAP Bind Requires Match of Operating Modes

Successful communication with an external user store depends on the following:

- The CA User Activity Reporting Module servers and their managing CA EEM server must be in the same FIPS mode, and
- The CA EEM server must be in the same FIPS mode as a FIPS-enabled external user store when using TLS v 1.0 for the connection.

  Note: FIPS-compatibility is not available when using unencrypted communications between the CA EEM server and the external user store, or when the CA EEM server and user store are in different FIPS modes.

SNMP Traps

You can send SNMP events using either SNMP V2 or SNMP V3. Both are supported in non-FIPS mode.

If the SNMP Trap Destination server is FIPS enabled you must choose V3 Security and then choose SHA as the authentication protocol and AES as the encryption protocol. You make these choices on the Destination page of the Schedule Action Alerts wizard.

Configure Microsoft Internet Explorer to Access CA User Activity Reporting Module in FIPS Mode

Your browser may require some additional configuration before it can display the CA User Activity Reporting Module server user interface when running in FIPS mode. Use the following procedure to set the required options to access CA User Activity Reporting Module in Microsoft Internet Explorer 7 or 8.

To configure Microsoft Internet Explorer 7 or 8

1. Open the browser and select the Tools, Internet Options.
2. Select the Advanced tab and scroll down to the Security section.
3. Select each of the following options:
   - Use SSL 2.0
   - Use SSL 3.0
   - Use TLS 1.0
4. Click OK.

Configure Mozilla Firefox to Access CA User Activity Reporting Module in FIPS Mode

Your browser may require some additional configuration before it can display the CA User Activity Reporting Module server user interface when running in FIPS mode. Use the following procedure to set the required options in Mozilla Firefox 3.5.8 or later browser to access a CA User Activity Reporting Module server running in FIPS mode.

Note: Access to CA User Activity Reporting Module requires installation of the Mozilla Firefox plug-in for Adobe Flash 9 or 10.

To configure Mozilla Firefox

1. Open the browser and select Tools, Options.
2. Click the Advanced tab and then click the Encryption subtab.
3. Select both of the following options:
   - Use SSL 3.0
   - Use TLS 1.0.
4. Select the Security subtab, and then select the option to use a Master Password.
5. Click Change Master Password... and provide a suitable password when the window appears, then click OK.
6. Select the Advanced subtab.
7. Click Security Devices.

   The Device Manager window appears.

8. Select the NSS Internal PKCS #11 Module in the left pane.

   This action populates the right pane.

9. Select the line, Module NSS Internal FIPS PKCS #11 Module, and click Enable FIPS.
10. Type the Master Password you created in a previous step when prompted, and then click OK.
11. Click OK in the Device Manager window.
12. Click OK in the Options window.
13. Restart the browser.

ISO Image for New Installations

To help you quickly deploy CA User Activity Reporting Module or to add a new CA User Activity Reporting Module server to an existing deployment, we are providing an ISO image for the service pack. The ISO image is available from the Downloads area on Support Online.

We recommend that you use the most recent ISO image in the following cases:

- Deploying CA User Activity Reporting Module. Installing from the latest ISO image minimizes the number of required subscription upgrades you must apply and speeds your deployment.
- Adding a new CA User Activity Reporting Module server after you have upgraded the servers in your existing deployment. First establish that the servers and agents in your current deployment are successfully upgraded and receiving events. Then install new servers using the ISO image to add more capacity and minimize the number of subscription updates to apply.

Note: The installation procedure has changed. A new prompt asks whether you want to install with FIPS mode enabled. When adding a new CA User Activity Reporting Module server to an existing FIPS deployment (the CA User Activity Reporting Module management server or remote CA EEM server are in FIPS mode), enable FIPS mode during the installation. Otherwise the new server cannot register and you must reinstall. See the *Implementation Guide* for more information about FIPS mode.

Chapter 16: New and Changed Features in r12.1

This section contains the following topics:

Open API Access

CA User Activity Reporting Module allows you to use API calls to access data from the event repository using the query and report mechanism, and display it in a web browser. You can also use the API to embed CA User Activity Reporting Module queries or reports in a CA or third-party product interface.

CA User Activity Reporting Module API features include:

- Authenticated, secure APIs
- Product registration for single sign-on (SSO)
- Retrieval of a query or report list, filtered by tag
- Display of a query or report in the interactive CA User Activity Reporting Module interface, allowing filtering, and embedding in a user interface

You can find more information about the API in the *API Programming Guide* and online help.

Actionable Alerts: CA IT PAM Integration

Through scheduled alerts that query volumes of log records, CA User Activity Reporting Module detects potential control violations and suspicious IT activity. CA User Activity Reporting Module notifies the IT security staff who investigates each alert to determine whether remediation action is required. Typical investigation activities are often routine and well-suited for automation. Through a tight integration between CA User Activity Reporting Module and CA IT PAM, these routine response actions can be performed automatically. IT security staff are free from repetitious tasks to focus on only the most important issues.

CA IT PAM integration lets you create requests in CA Service Desk by running a predefined CA IT PAM event/alert output process from alerts. You can also run custom IT PAM event/alert output processes from CA User Activity Reporting Module that automate other responses to suspicious events.

For details, see the "Working with CA IT PAM Event/Alert Processes" section in the Action Alerts chapter of the CA User Activity Reporting Module *Administration Guide*.

Actionable Alerts: SNMP Integration with NSM Products

Alerts are generated when scheduled queries retrieve events indicating suspicious activity. You can automate the sending of such alerts as SNMP traps to network security monitoring (NSM) products such as CA Spectrum or CA NSM. You prepare the destination products to receive and interpret SNMP traps from CA User Activity Reporting Module, configure the destination locations, then specify the event information to send.

For details, see the "Working with SNMP Traps" section in the Action Alerts chapter of the CA User Activity Reporting Module *Administration Guide*.

ODBC and JDBC Access

CA User Activity Reporting Module allows read-only access to collected event log information using ODBC and JDBC. You can use this access to do things like the following:

- Create customer reports using tools like BusinessObjects Crystal Reports
- Retrieve selected log information for use with a correlation engine
- Examine logs for intrusion or malware detection

The ODBC and JDBC access features use a client that you install on an appropriate server in your network. The CA User Activity Reporting Module server automatically installs its server-side components during subscription update and installation processing.

You can find installation information in the *Implementation Guide*. You can find configuration information and examples in the *Administration Guide*.

Identity and Asset Relevance: CA IT PAM Integration

CA IT PAM integration lets you maintain updated values for a given key by running a CA IT PAM dynamic values process. A dynamic values process is one that retrieves the current values from repositories that store current data. If you create a process that retrieves values for critical assets from your assets file or database, you can update the Critical_Assets key in predefined reports and queries with the click of a button.

For details, see the "Enabling Dynamic Values Import" section in the Queries and Reports chapter of the CA User Activity Reporting Module *Administration Guide*.

Extended Direct Log Collection by Default Agent

At the CA User Activity Reporting Module installation, the Syslog listener, named Syslog_Connector, is deployed on the default agent to enable the collection of syslog events. The Linux_localsyslog integration, with the associated connector, Linux_localsyslog_Connector, is also available to collect syslog events.

The default agent can now directly collect more than syslog events. Using the WinRm connector, the default agent can collect events from products running on Microsoft Windows platforms, such as Active Directory Certificate Services and Microsoft Office Communication Server. Using the ODBC connector, the default agent can collect events from multiple databases such as Oracle9i and SQL Server 2005, and applications that store their events in these databases.

Automated Update Schedules for Subscription Clients

When you install your first CA User Activity Reporting Module server, you configure global settings for all services, including subscription. For subscription purposes, the first server you install is the default subscription proxy. You configure the update start time and the frequency with which this proxy checks the CA Subscription Server for updates. When you install additional servers, they are installed as subscription clients, by default. When you configure additional servers, you do so at the local level. Configuration at the local level is done by selecting the name of the server to configure and then overriding selected global configurations.

By default, the update start time of subscription clients is inherited from the global setting. When the inherited setting is not overridden manually to force a delay, problems arise. To prevent this problem, the update schedule for clients is now automated with a 15 minute delay. The update schedule for subscription clients no longer requires manual configuration.

Chapter 17: Known Issues

This section contains the following topics:

Agents and CA Adapters

The following are the known issues related to agents and CA Technologies adapters.

Agentconfig Script Fails on AIX

Symptom:

The agenfconfig utility fails on AIX with a segmentation error.

Solution:

You can resolve this issue by exporting the following values before running the agentconfig utility:

```
export MALLOCMULTIHEAP=true
export AIXTHREAD_STK=756000
```

The Disable Non-CEG Event Data Option Fails on Agents

Symptom:

When you enable the Disable Non-CEG Event Data option in an upgraded environment, the corresponding tag is not updated on the agent.

Solution:

To resolve the issue, restart the agent.

centOS Agent Appears as RHEL5 in Connector Deployment Screens

Symptom:

The centOS agent does not appear to be available for use in connector deployment after download.

Solution:

The centOS agent appears by the proper name in the Download Agent Binaries list. Once you have downloaded it, it appears in deployment screens as "RHEL5". Select RHEL5 for the centOS agent.

Domain Level Event Source Configuration Fails

Symptom:

Configuring any connector to access a Windows event source and read its logs involves creating a low-privileged user account and assigning it the needed permissions. When the event source is a Windows Server 2003 SP1 host, one of the steps is to set the local security policy, *Impersonate a client after authentication*. When this user right is set locally, no problem occurs. However, if this setting is applied as a domain policy to all servers, the global application has the affect of removing the existing local assignments for other users, namely Administrators and SERVICE.

A Microsoft support article states that "... problems occur when a Group Policy setting that defines the Impersonate a client after authentication user right is linked to the domain. This user right should be linked only to a site or to an organizational unit (OU)."

Solution:

See the Microsoft Knowledge Base article ID 930220 for the recommendation to restore full unsecured TPC/IP connectivity by disabling the IPSec services and restarting the computer and the steps to add back the Administrators and SERVICE groups as a Group Policy setting. Try the following link:

http://support.microsoft.com/kb/930220

Microsoft also recommends the following methods to resolve problems caused by applying the setting Impersonate a client after authentication as a group policy:

- Method 1: Modify Group Policy settings
- Method 2: Modify the Registry

See the Microsoft Knowledge Base article ID: 911801 for the steps to implement both recommended resolutions. Try the following link:

http://support.microsoft.com/kb/911801

Limitation on Port Configuration

Symptom:

When the syslog listener is configured with the default UDP port on an agent running as a non-root user on a Linux host, UDP port 514 (default for syslog) is not opened and no syslog events are collected on that port.

Solution:

If the agent is running as a non-root user on a UNIX system, change the syslog listener ports to port numbers above 1024 or change the service to run as root.

Message Parsing Files Fail to Appear in Integration Wizard

Symptom:

After upgrading CA User Activity Reporting Module, when you open the integration wizard to edit an existing integration, or create a new one, Message Parsing files fail to appear. The XMP shuttle control where MP files normally appear is blank.

Solution:

You can increase the java heap size to eliminate this issue, and display MP files in the Integration Wizard.

1. Navigate to the iTechnology Directory at /opt/CA/SharedComponents/iTechnology and stop iGateway:

```
./S99igateway stop
```

2. Open the caelm-agentmanager.group file and locate the max heap size value as shown in bold in the following example:

```
<JVMSettings>
                <loadjvm>true</loadjvm>
                <javahome>/usr/java/latest/jre</javahome>
                <Properties
name="java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed" >

<system-properties>java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/en
dorsed</system-properties>
                </Properties>
                <Properties name="initial heap size" >
                        <jvm-property>-Xms512m</jvm-property>
                </Properties>
                <Properties name="max heap size" >
                        <jvm-property>-Xmx768m</jvm-property>
                </Properties>
        </JVMSettings>
```

3. Change the value as illustrated:

```
<jvm-property>-Xmx1024m</jvm-property>
```

4. Save and close the file, and restart iGateway:

```
./S99igateway start
```

OPSEC Connector Password Cannot Contain a "$"

Symptom:

When you apply an OPSEC connector in your environment, it fails with the following error:

```
[ConnectorFW::AddConnector] DllLoad Failed, Hence terminating the Connector
```

Solution:

The OPSEC password cannot contain the "$" character. Remove the character from the password and redeploy the connector.

Removing Server from Federation Does Not Remove Default Agent

Symptom:

When removing a CA User Activity Reporting Module server from a group of federated servers, the deleted server's default agent is not removed from its related agent group.

Solution:

Manually delete the agent from its group in the Agent Explorer sub-tab.

Reports with Data Collected from the CA SAPI Collector Are Not Displaying Events Properly

Symptom:

Events collected using the CA Audit SAPI Collector do not have all the event fields properly populated. This results in most of the reports not displaying the data in the expected manner.

Solution:

Use the CA Audit SAPI Router to collect events from your existing CA Audit infrastructure.

More information about configuring the SAPI Router is available in the *Implementation Guide* in the section, Considerations for CA Audit Users.

The Text File Log Sensor Running on a Solaris Agent System Stops Receiving Events

Symptom:

The Text File log sensor running on a Solaris agent system stops receiving events.

If you review the log file for the connector, it contains an error indicating that a library file, libssl.so.0.9.7, failed to open:

```
[4] 07/20/10 18:55:50 ERROR :: [ProcessingThread::DllLoad] :Error is: ld.so.1:
caelmconnector: fatal: libssl.so.0.9.7: open failed: No such file or directory [4]
07/20/10 18:55:50 ERROR :: [ProcessingThread::run] Dll Load and Initialize failed,
stopping the connector ...
[3] 07/20/10 18:55:50 NOTIFY :: [CommandThread::run] Cmd_Buff received is START
```

Solution:

Identify the location of the library to enable the agent to receive events.

To resolve the error on the Solaris agent system

1. Navigate to /etc folder. For example:

   ```
   cd /etc
   ```

2. Open profile file in the etc folder. For example:

   ```
   vi /etc/profile
   ```

3. Add the following two lines at the end of the profile file:

   ```
   LD_LIBRARY_PATH=/usr/sfw/lib:$LD_LIBRARY_PATH
   ```

   ```
   export LD_LIBRARY_PATH
   ```

4. Close the current session of the Solaris agent system.
5. Open a new session of the Solaris agent system.
6. Stop the CA User Activity Reporting Module agent on the Solaris system. For example:

   ```
   /opt/CA/ELMAgent/bin/S99elmagent stop
   ```

7. Start the CA User Activity Reporting Module agent on Solaris system. For example:

   ```
   /opt/CA/ELMAgent/bin/S99elmagent start
   ```

   The Text File log sensor starts receiving events and the error is no longer displayed in the log file.

Very High Event Flow Causes the Agent to Become Unresponsive

Symptom:

A CA User Activity Reporting Module agent becomes unresponsive and stops accepting events. The following error message appears in the caelmdispatcher.log file:

```
[275] 07/12/10 14:32:05 ERROR :: FileQueue::PutEvents Unable to write to new event file
[275] 07/12/10 14:32:05 ERROR :: WriterThread::run Unable to push events to FileQueue, Retrying
[275] 07/12/10 14:32:10 NOTIFY :: FileQueue::UpdateCurrentWriterFile Reached Max files configured limit=10, Not creating any new files for now
```

Solution:

This indicates that there is a very high rate of incoming events for the hardware in the environment. You can address this issue by reconfiguring the agent, using the following procedure:

1. Click Administration, the Log Collection subtab, and expand the Agent Explorer folder.
2. Select the agent you want to reconfigure, click Edit, and adjust the following parameters:

   Max Number of Files

   Sets the maximum number of files that can be created in the event reception file queue. The Max Number limit is 1000 files. The default setting is 10.

   Max Size per File

   Sets the maximum size, in MB, for each file in the event reception file queue. When a file reaches the maximum size, CA User Activity Reporting Module creates a new file. The Max Size limit is 2048 MB. The default setting is 100 MB.

   You can adjust these parameters upwards as required by your environment and event per second rate.

CPU Throttling Is Not Supported on HP-UX PA-RISC and HP-UX Itanium Agents

Symptom:

When you enable the CPU throttling feature on machines that run the HP-UX PA-RISC and HP-UX Itanium agents, the CPU usage is not throttled.

Solution:

CA User Activity Reporting Module 12.5.03 does not support the CPU throttling feature on machines that run the HP-UX PA-RISC and HP-UX Itanium agents.

The Agent Stops When Redirecting the Agent on Solaris

Symptom:

When you use the agentconfig utility to redirect the CA User Activity Reporting Module agent on Solaris, the CA User Activity Reporting Module agent stops and does not restart.

Solution:

You can resolve this issue by restarting the agent.

Appliance (non-UI)

The following are the known issues related to the soft-appliance (not the CA User Activity Reporting Module user interface).

Cannot Log into CA User Activity Reporting Module Server Using EiamAdmin User Name

Symptom:

EiamAdmin user name and password are not recognized when trying to log into the CA User Activity Reporting Module server (not through the user interface).

Solution:

To perform maintenance-related tasks, such as configuring archiving, the installation creates another user name, caelmadmin, and assigns it the same password as the installer provided for EiamAdmin. Use the caelmadmin user name and password to log into the CA User Activity Reporting Module server.

For more information, see Default User Accounts in the *Implementation Guide*.

Event Correlation

The following are the known issues related to event correlation.

Correlation Ignores Events Marked Ahead of the Server Time

Symptom:

The correlation engine ignores events with timestamps more than 5 minutes ahead of the CA User Activity Reporting Module server time.

Solution:

Such events are not considered for incident inclusion, regardless of the Correlation Event Span values.

Correlation Service Fails to Initialize on Startup

Symptom:

The correlation engine fails to initialize on startup. When this happens CA User Activity Reporting Module generates a Correlation Service log entry, and a self-monitoring event with the following text:

```
Unable to initialize service CorrelationService: java.lang.RuntimeException:
com.ca.elm.common.repository.RepositoryException: Error authenticating to EEM
<hostname>
```

Solution:

To resolve this issue, restart ELM Services using the following procedure:

1. Click the Administration tab, then the Services subtab, and expand the System Status node.
2. Select the CA User Activity Reporting Module server where you want to restart services.
3. Click Restart Services.

Correlation Rule Filters Fail to Identify Incident Events

Symptom:

An event correlation rule filter fails to identify events as expected when using wildcards. For example, a rule set to match the value "test*" does not return values beginning with "test", such as "testa"

Solution:

The correlation engine uses strict regular expression syntax as regards wildcards. So in this example, you would have to use "test.*" to return the results you want.

Line Break Does Not Function in Correlation Wizard Fields

Symptom:

In certain correlation rule field wizards, a line break cannot be created using "</BR>" This issue applies to the following fields:

- Incident Descripton in the Details step
- Incident Remediation in the Details step
- Subject in the Email tab of the Notifications step
- Text in the Email tab of the Notifications step

Solution:

The "<" character is not currently allowed in the listed fields, so the line break cannot be entered.

Event Refinement

The following are the known issues related to event refinement.

Block Mapping String and Numeric Values Require Different Operators

Symptom:

When using the Mapping Wizard, block mapping values for numeric or text string columns do not respond as expected.

Solution:

When creating block mappings, the ‘Equal’ operator can only be used with numeric columns. Use the ‘Match’ operator for all text string columns.

Message Parsing Rules Produce an Error When Modified

Symptom:

If you copy the rules from subscription and try to modify their content, an error occurs.

Solution:

This error occurs because the content in the rules is unordered in a subscription. If you want to modify a rule, you must reposition the rules.

If a rule requires a mapping variable of a mapping block, you must define the mapping variable before you use it in either that mapping block or its preceding mapping block. The following is the order of precedence of the mapping blocks:

1. Direct Mapping
2. Functional Mapping
3. Conditional Mapping
4. Block Mapping

Queries and Reports

The following are the known issues related to queries and reports.

Event Data With Non-UTF8 Characters Does Not Display in XML or PDF

Symptom:

Query or report results that contain non-UTF8 characters cannot be exported to XML or PDF formats. This issue applies only to events collected before updating to r12.5.

Solution:

Non-UTF8 characters in historical event data causes XML parsing to fail, which also prevents PDF export. Historical data without non-UTF8 characters exports properly to XML and PDF.

You can also export event data containing non-UTF8 characters as an MS Excel spreadsheet.

Query and Reports Pages Are Displaying Error Messages When the UI is Loading

Symptom:

When a CA User Activity Reporting Module server is loading the Queries and Reports pages, the following error is displayed on the UI:

```
Error getting query/report results: HTTP request error
```

Solution:

This error occurs if you have used a medium configuration for collection and reporting servers using CA User Activity Reporting Module as a virtual appliance. In a Hub and Spoke model, we highly recommend that you use a medium deployment configuration for a collection server and a large deployment configuration for a reporting server.

Queries and Reports Fail to Find Host

Symptom:

When you run queries or reports, the following error appears:

```
Error getting query results: Run Query: Host does not exist
```

Solution:

This error occurs when you launch a query or report after restarting the igateway, but before UI spindle initialization is complete. Wait at least 5 minutes after restarting igateway before running queries or reports. The delay allows the initialization to finish.

Subscription

The following are the known issues related to subscription.

Keyed List Updates Disabled After Upgrade

Symptom:

Scheduled keyed list upgrades are disabled after you upgrade to release 12.5.02 using the subscription system.

Solution:

If you had scheduled keyed list upgrades enabled before the upgrade, you can simply reenable them from the Alerting Service interface screen.

Offline Subscription Files Are Unavailable on Offline Proxy

Symptom:

After upgrading to CA User Activity Reporting Module version 12.5, and manually installing an offline susbcription package on an offline proxy server, you cannot access the offline package through the CA User Activity Reporting Module user interface. In Subscription Service Configuration for the offline server, when you choose the offline package in the File dropdown, and click Browse, a timeout message appears.

Solution:

A .jar file in the IGW folder of the proxy server needs to be deleted. To delete the file, do the following:

1. On the proxy server, navigate to the $IGW_LOC directory.
2. Stop igateway using the command

   ./S99igateway stop
3. Delete the file subscription.jar using the command

   rm -rf Subscription.jar
4. Start igateway using ./S99igateway start.

Subscription Schedule is Reset after Upgrading the Subscription Server

Symptom:

When you configure the schedule for a subscription update, the schedule is reset after the subscription server is upgraded. The subscription clients are not upgraded.

Solution:

You can resolve this issue by performing the following steps:

1. Select each subscription client you want to upgrade.
2. Click Upgrade Now.

User and Access Management

The following are the known issues related to user and access management.

Custom Administrators Not Confined by Access Policies

Symptom:

If you create a custom administrator and assign users to that administrator, attempts to set access policies to confine the custom administrator to viewing only those users fails. A custom administrator can view any user regardless of identity access policy.

Solution:

This behavior occurs due to a user store management issue. You cannot presently create a custom administrator with rights to view only a certain subset of users.

Limitation on Calendar Use with Access Policies

Symptom:

You have limited user or group access to CA User Activity Reporting Module during the times and days specified on a calendar with a policy that explicitly grants access. However, the calendar does not function as expected with a policy that explicitly denies access.

Solution:

Use the explicit grant policy type to limit the times you want to grant a group access rather than using an explicit deny policy.

Virtualization

The following are the known issues related to virtualization.

VAPP Provisioning on ESX Server Fails

Symptom:

Provisioning the CA User Activity Reporting Module VAPP for 12.5.02 fails with the following error:

```
Error: Host CPU is incompatible with the virtual machine's requirements at CPUID level 0x8000001 register 'edx'
```

Solution:

This error occurs when the host VT (Virtualization Technology) is not enabled. To resolve the issue, enable VT in BIOS for the ESX server before provisioning. Consult your host computer hardware documentation for information on enabling VT in your environment.

Performance Problems on ESX Server

Symptom:

When running CA User Activity Reporting Module in an ESX environment you may encounter performance problems. These problems can apply to CA User Activity Reporting Module, as well as other virtual application servers running on the same ESX server.

Solution:

This issue has been resolved in some cases by installing VMware tools on the CA User Activity Reporting Module appliance. VMware tools is not officially supported, so this solution may not work in all environments.

Miscellaneous

The following are the miscellaneous known issues.

CA User Activity Reporting Module Is Sometimes Non-Responsive

Symptom:

Sometimes CA User Activity Reporting Module is non-responsive. That is, the user interface does not respond to user requests and internal requests from the agent to agent manager stop. However, log collection continues.

Solution:

Use the following procedure to stop the iGateway process and restart it:

1. Log on to the non-responsive CA User Activity Reporting Module server through ssh as the caelmadmin user.
2. Switch users to the root account with the following command and provide the root password:

   ```
   su -
   ```

3. Navigate to the $IGW_LOC directory.

   By default, iGateway resides in the directory, /opt/CA/SharedComponents/iTechnology.

4. Stop the iGateway process with the following command:

   ```
   ./S99igateway stop
   ```

5. Start the iGateway process with the following command:

   ```
   ./S99igateway start
   ```

Events Export to PostgreSQL Fails with Fatal Error

Symptom:

When you export events to PostgreSQL using the DBExport utility, the following error is displayed in the self-monitoring events:

```
FATAL: sorry, too many clients already
```

Solution:

To resolve the issue, restart the PostgreSQL service.

Custom ODBC Database Connection Fails

Symptom:

A custom connection set up to allow you to query an ODBC database fails.

Solution:

This issue occurs when ODBC Schema names are entered in lower-case letters during configuration. Make sure that when you configure an ODBC connection in the Report Service interface, you enter any schema names in all capital letters.

Display Time is Wrong

Symptom:

Display time is wrong after CA User Activity Reporting Module server is provisioned using the Virtual Appliance.

Solution:

Use the following workaround to resolve this issue:

1. Stop the iGateway.
2. Set the display time manually.
3. Restart the iGateway.

Event Collection Profiles Fail to Appear on Upgrade

Symptom:

After you upgrade to the 12.5.02 release from a previous release, subscription Event Collection Profiles fail to appear in the user interface.

Solution:

This issue occurs when the Content upgrade module is not the final module installed. To resolve the issue, repeat the upgrade process with only the Content module selected. When the content-only upgrade is complete, the Event Collection profiles appear properly.

More information:

Upgrading to CA User Activity Reporting Module Version 12.5 through Subscription (see page 13)
Upgrading to CA User Activity Reporting Module Version 12.5 through Offline Subscription (see page 17)

High Contrast Settings for Monitor

Symptom:

In Windows, the only supported high contrast setting is High Contrast Black; the other three high contrast options are not supported. High contrast options include High Contrast #1, High Contrast #2, High Contrast Black, and High Contrast White.

Solution:

Select the High Contrast Black setting, when a high contrast setting is needed. To set this option, select Display from the Control Panel. This accessibility option is set on the Display Properties dialog, Appearance tab, Color scheme drop-down list.

iGateway Continuously Stopping and Restarting

Symptom:

The CA User Activity Reporting Module interface occasionally stops responding during operations. Checking the CA User Activity Reporting Module server reveals that the iGateway process is stopping and restarting but failing to stay up. Use the following process to check the iGateway process:

1. Access a command prompt on the CA User Activity Reporting Module server.
2. Log in with the caelmadmin account credentials.

3. Switch users to the root account with the following command:

   ```
   su - root
   ```

4. Use the following command to verify that the iGateway process is running:

   ```
   ps -ef | grep igateway
   ```

   The operating system returns the iGateway process information and a list of processes running under iGateway.

Solution:

Use the following workaround to resolve the problem:

1. Go to $IGW_LOC (/opt/CA/SharedComponents/iTechnology), and locate the following file:

   ```
   saf_epSIM.*
   ```

   There are multiple versions, numbered sequentially, for example, saf_epSIM.1, saf_epSIM.2, saf_epSIM.3, and so on.

2. Rename the lowest-numbered file and save it in another location for transmission to CA Technologies support.
3. If iGateway does not automatically restart, restart it:
   a. Log in as the root user.
   b. Access a command prompt and enter the following command:

      ```
      /opt/CA/SharedComponents/iTechnology/S99igateway start
      ```

Keyed Lists Configured Locally Fail to Appear After Upgrade

Symptom:

After upgrading to CA User Activity Reporting Module version r12.5, when you examine the available Keyed Value list under Administration > Library > Keyed Lists > Subscription, some Keyed Values no longer appear.

Solution:

In CA User Activity Reporting Module version r12.5, Keyed Value lists have been moved from Services to Library, under Administration. If you had previously specified a Keyed Value as local to a specific server, rather than global for your entire CA User Activity Reporting Module environment, that Keyed Value is not retained after upgrade to version r12.5.

To avoid losing Keyed Values, before upgrading to version r12.5, set all Keyed Values to global configuration.

Max Disk Space for Virtual CA User Activity Reporting Module Is Too Small

Symptom:

Not able to create a virtual machine with an allocated disk space of 512 GB in VMware ESX Server v3.5. My virtual CA User Activity Reporting Module server needs more than the 256 GB maximum to handle event volume.

Solution:

VMWare ESX Server uses a default Block Size of 1 MB, and calculates the maximum disk space using this value. When the block size is set to 1 MB, the maximum disk space defaults to 256 GB. If you want to configure more than 256 GB of virtual disk space, you can increase the default block size.

To create a larger virtual disk

1. Access the service console on the VMware ESX Server.
2. Increase the Block Size to 2 MB with the following command:

   ```
   vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   In this command, the value 2M means 512 GB (2 x 256).
3. Restart the VMware ESX Server.
4. Create a new virtual machine with disk space set to 512 GB.

More information about this command and other commands is available in the VMware ESX Server documentation.

Out of Memory Error on Machines with Low Memory

Symptom:

The download of a subscription update to a computer with less than the recommended 8 GB of memory fails with a Java out of memory error.

Solution:

If you install CA User Activity Reporting Module on hardware with less than the recommended 8 GB of memory, change the JVM heap size setting by editing the caelm-java.group file.

To change the JVM heap size setting

1. Log on to the CA User Activity Reporting Module server as caelmadmin.
2. Navigate to the iGateway folder.

3. Open the caelm-java.group file and locate the the JVM settings section.
4. Add the new line, as shown in the following illustration in bold:

```
<JVMSettings>
                <loadjvm>true</loadjvm>
                <javahome>/usr/java/latest/jre</javahome>
                <Properties
name="java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed">

<system-properties>java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/en
dorsed</system-properties>
                </Properties>
        <Properties
name="maxmemory"><jvm-property>-Xmx1250M</jvm-property></Properties>
        </JVMSettings>
```

5. Save and close the caelm-java.group file

Important! Setting the JVM heap size can cause problems when using the Export to PDF option with large data sets. Thus, this option is best used on only small computers, which run with less than the recommended RAM and processing power.

Refreshing Browser Logs User Out of CA User Activity Reporting Module

Symptom:

Refreshing your browser while logged in to CA User Activity Reporting Module ends your session, logging you out.

Solution:

CA User Activity Reporting Module does not support browser refresh because of Flex limitations. Avoid refreshing your browser.

EE_POZERROR Repository Error Appears on Login When Using Remote EEM

Symptom:

When you open the CA User Activity Reporting Module interface in an environment using a remote EEM server, the interface may fail to display properly. Instead an "EE_POZERROR Repository Error" appears.

Solution:

Close and reopen the browser to resolve the issue.

Screen Captures May Show CA User Activity Reporting Module Title

Screen captures inlcuded in the 12.5.02 release documentation may show the CA Enterprise Log Manager title, rather the the CA User Activity Reporting Module title. This change is purely cosmetic. Navigation and functionality are unchanged.

Service or Explorer Interface Error May Occur After iGateway Restart

Symptom:

If you click on an object in the CA User Activity Reporting Module interface services or explorer trees immediately after an iGateway restart, you may see an error message reading "Network error on receive" rather than the requested content.

Solution:

This error occurs if you attempt to access one of the specified objects while they are still being reloaded after the iGateway restart. Wait five minutes to allow the reload to finish and click the services or explorer item you want.

Uploads and Imports Fail with any Non-IE Browser

Symptom:

When you browse to CA User Activity Reporting Module with Mozilla Firefox, Safari, or Chrome, you can perform most CA User Activity Reporting Module tasks successfully. However, any upload or import tasks fail when using any of these browsers. Examples follow:

- Importing a query definition fails with an "IO Error: Request Failure" message.
- Uploading a CSV file with the bulk connector deployment wizard fails, despite the message, "Uploading file."

Solution:

Browse to CA User Activity Reporting Module with Microsoft Internet Explorer when you want to upload or import files.

User Interface Unexpectedly Fails to Display Properly on Installation with Remote EEM

Symptom:

When installing CA User Activity Reporting Module with a remote EEM server, the user interface occasionally fails to display properly on initial login. Reviewing the iGateway log files reveals that the agentmanager, calmreporter, subscclient and subscproxy services have not started.

You may see log file syntax similar to this:

```
[1087523728] 09/23/09 20:35:32 ERROR :: Certificate::loadp12 : etpki_file_to_p12
failed [ errorcode : -1 ]

[1087523728] 09/23/09 20:35:32 ERROR :: Certificate::loadp12 : etpki_file_to_p12
failed [ errorcode : -1 ]

[1087523728] 09/23/09 20:35:32 ERROR :: Certificate::loadp12 : etpki_file_to_p12
failed [ errorcode : -1 ]

[1087527824] 09/23/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process for
SponsorGroup [ caelm-msgbroker ] didn't respond OK for the termination call

[1087527824] 09/23/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process for
SponsorGroup [ caelm-oaserver ] didn't reaspond OK for the termination call

[1087527824] 09/23/09 17:00:07 ERROR ::
OutProcessSponsorManager::stopSponsorGroup : terminating safetynet process for
SponsorGroup [ caelm-sapicollector ] didn't reaspond OK for the termination call

[1087527824] 09/23/09 17:07:46 ERROR :: OutProcessSponsorManager::start :
SponsorGroup [ caelm-java ] failed to start ]

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
agentmanager ] failed to load

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
calmreporter ] failed to load

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscclient ] failed to load

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [
subscproxy ] failed to load
```

Solution:

You can resolve this problem by restarting iGateway, and logging in to the interface again.

To restart the iGateway service

1. Click the Administration tab and then click the Services subtab.
2. Expand the System Status entry.
3. Select a specific CA User Activity Reporting Module server.
4. Click the service's Administration tab.
5. Click Restart iGateway.

Upgrade to 12.5.x From Earlier Versions Fails

Symptom:

When you update CA User Activity Reporting Module from a release before 12.5.0 to release 12.5.0 or later using the CA User Activity Reporting Module subscription system, you may experience errors or upgrade failure.

Solution:

To avoid these errors, you can manually install the 12.5 preupgrade package, using the following procedure. This procedure can be used for both Subscription and Offline upgrades. It replaces the preupgrade package installation procedures described in the appropriate sections of this document.

To install the CA User Activity Reporting Module 12.5.x preupgrade package manually

1. Navigate to the FTP offline subscription site:

   ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription

   The directory index displays a folder for each CA User Activity Reporting Module release.
2. Select the 12.5.xx_Offline_Subscription folder, and the Pre_12.5_Upgrade folder.
3. Download the pre-12.5 offline subscription update package. The file name follows the following format:

   subscription_12_5_xx_yy.tar
4. Using physical media such as a disk, or using scp, manually copy the .tar file to the CA User Activity Reporting Module appliance. We recommend a partition with a large amount of available space, such as /data/temp.
5. Untar the subscription file in your chosen directory.

   The main .tar file package contains four update.zip files:

   - iGateway
   - Java
   - EEM
   - ELM binary
6. Manually open each of these zip files using jar -xf. You can do so in any order, but the ELM binary package must be last.

   Each zip file contains an update shell script that installs the contents of the package. For example, EEM_update.sh
7. Locate and run each of these update scripts, ending with the ELM update, Upgrade_Server.sh.

   A message containing the target update version appears.

8. Enter yes to continue, and wait for the upgrade to complete.

   Return to the CA User Activity Reporting Module interface to confirm the upgrade.

When you have finished this procedure, you can complete your Subscription upgrade (see page 13) or Offline upgrade (see page 17).

An Undefined Server Name Replaces the Primary CA User Activity Reporting Module Server Name

Symptom:

When you deploy CA User Activity Reporting Module as a virtual appliance, the name of the primary CA User Activity Reporting Module server is displayed as ca-elm on the Subscription Dashboard.

Solution:

You can resolve this issue by performing the following steps:

1. Click the Administration tab, the Services subtab, and the Subscription Service folder.

   The Global Service Configuration: Subscription Service page is displayed.
2. Type the name of the primary CA User Activity Reporting Module server in Default Subscription Proxy.
3. Select the name of the primary CA User Activity Reporting Module server from the Subscription Proxy(s) for Client Updates.
4. Select the name of the primary CA User Activity Reporting Module server from the Subscription Proxy(s) for Content Updates.
5. Click Save.

DSN Creation Fails on a Windows 64-bit Machine

Symptom:

When you install the ODBC DataDirect installer on a 64-bit machine, you cannot add a DSN from the ODBC Data Sources.

Solution:

You can resolve this issue by performing the following steps:

1. Navigate to C:\Windows\sysWOW64\odbccad32.dll.
2. Add the DSN.

The Path /opt/CA/LogManager/help Contains Connector Guides for Unsupported Integrations

Symptom:

The path /opt/CA/LogManager/help contains connector guides for integrations that are not supported in CA User Activity Reporting Module 12.5.03 and later versions.

Solution:

CA User Activity Reporting Module 12.5.03 and later versions support limited integrations to align with the Identify and Access Management strategy, so the UI displays the connector guides for only the supported integrations. However, the path /opt/CA/LogManager/help contains the connector guides for unsupported integrations too because CA User Activity Reporting Module stores the connector guides for all the integrations supported by CA User Activity Reporting Module 12.0 through 12.5.04 in /opt/CA/LogManager/help.

CPU Throttling is not Functioning

Symptom:

When you configure the CPU throttling feature after you upgrade the CA User Activity Reporting Module server to CA User Activity Reporting Module 12.5.04, the CPU throttling feature does not function.

Solution:

This issue occurs if you upgrade only the CA User Activity Reporting Module server but you do not upgrade the CA User Activity Reporting Module agent. If you upgrade only the CA User Activity Reporting Module server, you can configure the CPU throttling feature but CA User Activity Reporting Module agent does not support the feature.

LogSensors and Listeners

The following are the known issues related to the logsensors and listeners.

Repeated Events Appear in CA User Activity Reporting Module

Symptom:

CA User Activity Reporting Module receives repeated events when you reboot the event source computer from which the WMI logsensor is receiving events.

Solution:

This is a known issue. A fix for this issue will be available in a future release of CA User Activity Reporting Module.

User Credentials Authentication Fails on WMI LogSensor

Symptom:

CA User Activity Reporting Module fails to authenticate a user when you deploy a WMI logsensor to receive events from a local computer. The WMI logsensor is able to receive events from the local computer.

Solution:

This is default behavior. Microsoft Windows does not validate user credentials when you deploy a WMI logsensor on the local computer.

Connector Deployment Fails for a Cisco Router Integration

Symptom:

When you deploy a connector using the syslog listener for Cisco Router 12.1 or Cisco Router 12.2 integrations, the connector deployment fails intermittently.

Solution:

This is a known issue. A fix for this issue will be available in a future release of CA User Activity Reporting Module.

The Syslog Listener Restarts at Regular Intervals

Symptom:

When you enable the CPU throttling feature on Solaris computers, the syslog listener restarts at regular intervals.

Solution:

You can resolve this issue by disabling the CPU throttling feature.

Deployment of Connector Based on the Local Syslog LogSensor Fails on RHEL 6 32-bit Machines

Symptom:

When I deploy a connector that is based on the local syslog logsensor on an RHEL 6 32-bit machine, the deployment fails.

Solution:

To resolve the issue, update the path in Syslog conf File Path of the connector configuration page from /etc/syslog.conf to /etc/rsyslog.conf.

Chapter 18: Fixed Issues

This section contains the following topics:

Issues List

The following customer-reported issue have been fixed in this release:

- 21394952/2
- 21421092/2
- 21441286/1
- 21494006/2
- 21494006/3
- 21531848/1
- 21361521/3
- 21370446/3
- 21524877/2

Chapter 19: Documentation

This section contains the following topics:

Bookshelf

The Bookshelf provides access to all CA User Activity Reporting Module documentation from a central location. The Bookshelf includes the following:

- Single expandable list of contents for all guides in HTML format
- Full text search across all guides with search terms highlighted in the content and ranked search results

  Note: When searching for purely numeric terms, precede the search value with an asterisk.
- Breadcrumbs that link you to higher level topics
- Single index across all guides
- Links to PDF versions of guides for printing

How to Access the Bookshelf

CA product documentation bookshelves are available for download in ZIP files titled All Guides Including a Searchable Index.

To access the CA User Activity Reporting Module bookshelf

1. Go to Search Documentation / Guides.
2. Type CA Enterprise Log Manager for the product, select a release and language and click Go.
3. Download the ZIP file to your desktop or other location.
4. Open the zip file and drag the bookshelf folder to your desktop or extract it to another location.
5. Open the bookshelf folder.
6. Open the bookshelf:
   - Open Bookshelf.hta if the bookshelf is on the local system and you are using Internet Explorer.
   - Open Bookshelf.html if the bookshelf is on a remote system or if you are using Mozilla Firefox.

   The bookshelf opens.

Appendix A: Acknowledgements

This appendix lists the third-party software used in CA User Activity Reporting Module for which licensing agreement information has been provided. The following third-party software are used in [set to your product name]:

Note: To view the licensing agreement information for a third-party software in HTML format, click Third Party Software Acknowledgements. To view the licensing agreement information for a third-party software in text format, see the third_party_software_acknowledgements file in the \\CA UARM 12.6\Bookshelf_Files\TPSA folder.

- Adaptive Communication Environment (ACE) 5.5.10
- Adobe Flex SDK 3.5
- Ant 1.6.5
- Boost 1.39.0
- CentOS 5.8
- Connector for ODBC 6 SP1
- DataDirect OpenAccess 6.0
- dom4j 1.6.1
- Formatting Objects Processor (FOP) 0.95 and FOP 1.0
- Google Protocol Buffers 2.3.0
- Jackson 1.7.4
- Jakarta POI 3.0
- Java Caching System (JCS) 1.3
- Jaxen 1.1
- JAXP 1.2.0-FCS
- JDOM 1.0
- Jersey 1.5

- Log4cplus 1.0.2
- Log4j 1.2.15
- PCRE 8.1
- POI 3.0
- POI 3.6
- Postgres JDBC driver 9.3
- Qpid 0.5.0
- Qpid 0.6.0
- Quartz 1.5.1
- Red Hat Enterprise Linux 5.5
- SQLite JDBC 3.7.15
- SQL Server JDBC Driver 4.0
- SNMP4J 1.9.3d
- Sun JDK 1.6.0_19
- Sun JDK 1.6.0_25
- Super CSV 1.52
- Tomcat 7.0.40
- Xerces-C 2.6.0
- XMLBeans 2.5.0
- Zlib 1.2.3
- ZThread 2.3.2

Appendix B: Accessibility Features

CA Technologies is committed to ensuring that all customers, regardless of ability, can successfully use its products and supporting documentation to accomplish vital business tasks. This section outlines the accessibility features that are part of CA User Activity Reporting Module.

Accessibility Mode

You can set CA User Activity Reporting Module to use an accessibility mode, which displays all graphic panels in queries and reports as tables instead. To enter accessibility mode, select the Activate Accessibility check box on the login screen.

Accessibility Controls

You can use keyboard controls to navigate through CA User Activity Reporting Module, as shown in the following table:

Tasks	Keyboard Controls
Switch between open applications	CTRL-TAB
Select a file in a open window	CTRL-TAB
Help	F1
Button Click	Space or Enter
Check Box Selection	Space or Enter
Open Menu, Combo Box	CTRL + Down Arrow
List Navigation	CTRL + Down Arrow to set focus Up/Down arrows to navigate Space or Enter to select list item
Radio Button Group	CTRL + Down Arrow to set focus Up/Down arrows to navigate Space or Enter to select list item
Close Active Window	ALT F4
Double-click	CTRL + D