Orchestria®

Deployment Overview

Orchestria Active Policy Management

Version 6.0

Copyrights

Disclaimer

Every effort has been made to ensure that this document accurately describes the operation of Orchestria APM. However, Orchestria does not accept any responsibility for the consequences of any discrepancies between the description of Orchestria APM contained in this manual and the Orchestria APM system as implemented.

Orchestria also reserves the right to make amendments to the contents of this manual from time to time to reflect changes made to the specification of Orchestria APM or for any other reason.

Trademarks

Contents

chapter 1
Introduction

This manual provides an overview of the deployment process for Orchestria Active Policy Management (APM). Such deployments can be very complex, and vary from one organization to the next. This chapter summarizes the product architecture, illustrating in simple terms how the various product components and features can connect to each other. For details, see:

- Client machine deployments, on page 6
- Content services, on page 7
- Integration with e-mail archives, on page 8
- Importing IM conversations, on page 9
- Policy engines, on page 10
- iConsole, on page 11
- Quarantine Manager, on page 12

Chapter 2, Deployment tasks, maps a route through the overall Orchestria APM deployment process, plotting each major task, and then breaking each major task down into a series of installation or configuration steps. Where necessary, individual steps include a cross-reference to sources of further information.

Contact us

To contact the service desk, go to:

http://support.orchestria.com

If you do contact the service desk, they may ask you to supply the following log files:

- The infrastructure log file, `wgninfra.out`.
- Any relevant system log files. These take the format: `stderr_200201200945.log`.

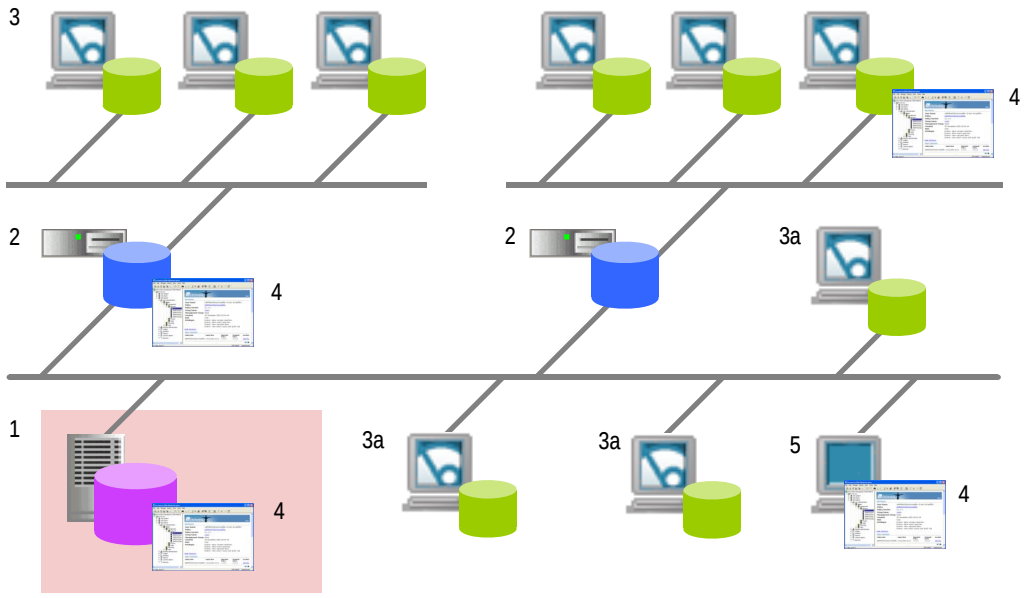
Find these files in Orchestria's \data\log subfolder of the Windows All Users profile; see the Administrator guide; search the index for 'logfiles'.

Client machine deployments

Orchestria APM deployments can be complex, and vary from one organization to the next. This section shows the architecture for a simple deployment to client machines. This enables you to install Orchestria APM client agents on users' desktops to monitor and control their e-mail and Web activity.

Here, Orchestria APM machines are organized into hierarchical branches, with the central management server (CMS) as the top level server. Below the CMS, each branch of the hierarchy is optionally managed by a gateway, and each gateway can serve multiple client machines and/or further gateways. You manage Orchestria APM using consoles. You can deploy consoles on any machine in your Orchestria APM installation.

Note that client machines and gateway servers are optional. Alternative 'server only' deployments may just include a CMS plus machines hosting Content Services components, Event Import components, and/or policy engines (see pages 7 to 10). Alternatively, you can have a 'hybrid' deployment, incorporating both client machines and these additional components.



Orchestria APM example architecture

1 CMS: This is the central repository for your Orchestria APM installation, holding all policy details and captured data.

2 Gateway: These are data-routing servers, operating between the CMS and client machines. They provide resilience and network load balancing. Each gateway can server multiple client machines or even child gateways.

3 Client machines: These run Orchestria APM e-mail and Web integration features (the 'client agents'). If required, client machines can connect directly to the CMS (3a) with no intermediate gateway.

4 Console: Any Orchestria APM machine can run any combination of Administration console, Data Management console, and Executive console.

5 Console-only machine: No Orchestria APM server software or client integration features are installed on this machine.

Content services

Orchestria APM Content Services provide access to the Content Search and Content Agent features. Based on innovative pattern-matching technology and intelligence contained in the Content Database, these features give you the ability to capture, control, or search for e-mails or Web events based on their text content. Content Services can be based on underlying FAST technology. For details, see the Deployment guide; search the index for 'content services'.

FAST-based deployments

FAST supports single and multi node deployments. In a single node deployment, all functional services are installed on a single host machine. In a multi node deployment, FAST services distributed across multiple host machines.

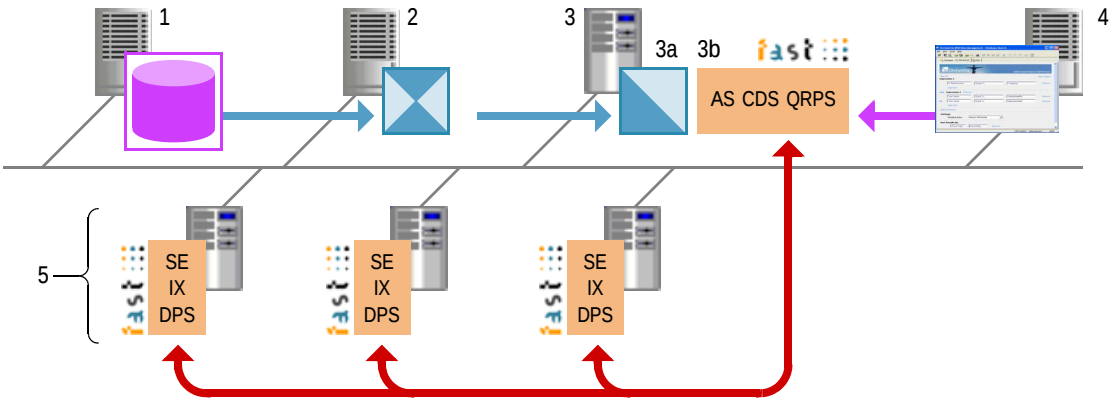
Single node or multi node deployments?

The decision to opt for a single or multi node deployment depends on various factors, including: the rate at which you need to input documents into the FAST system; the size and type of the documents; which documents need to be available for searching; and the availability of computing hardware. However, FAST systems are engineered for in-built scalability, and so distributing document processing and query handling over multiple host machines improves indexing performance and provides resilience and fault tolerance.

Example multi node deployment

You must plan multi node deployments very carefully. In particular, you must consider how many machines you need and how the deployment will impact on your network. A simplified example is shown below, comprising a single 'admin node' and three 'search and indexing nodes'.

All events submitted by the Orchestria APM content indexer are assigned, by the FAST content distributor on the admin node, to one of the FAST document processors running on a search and indexing node. All content searches generated in an Orchestria APM Data Management console are handled by the query results processor on the admin node.



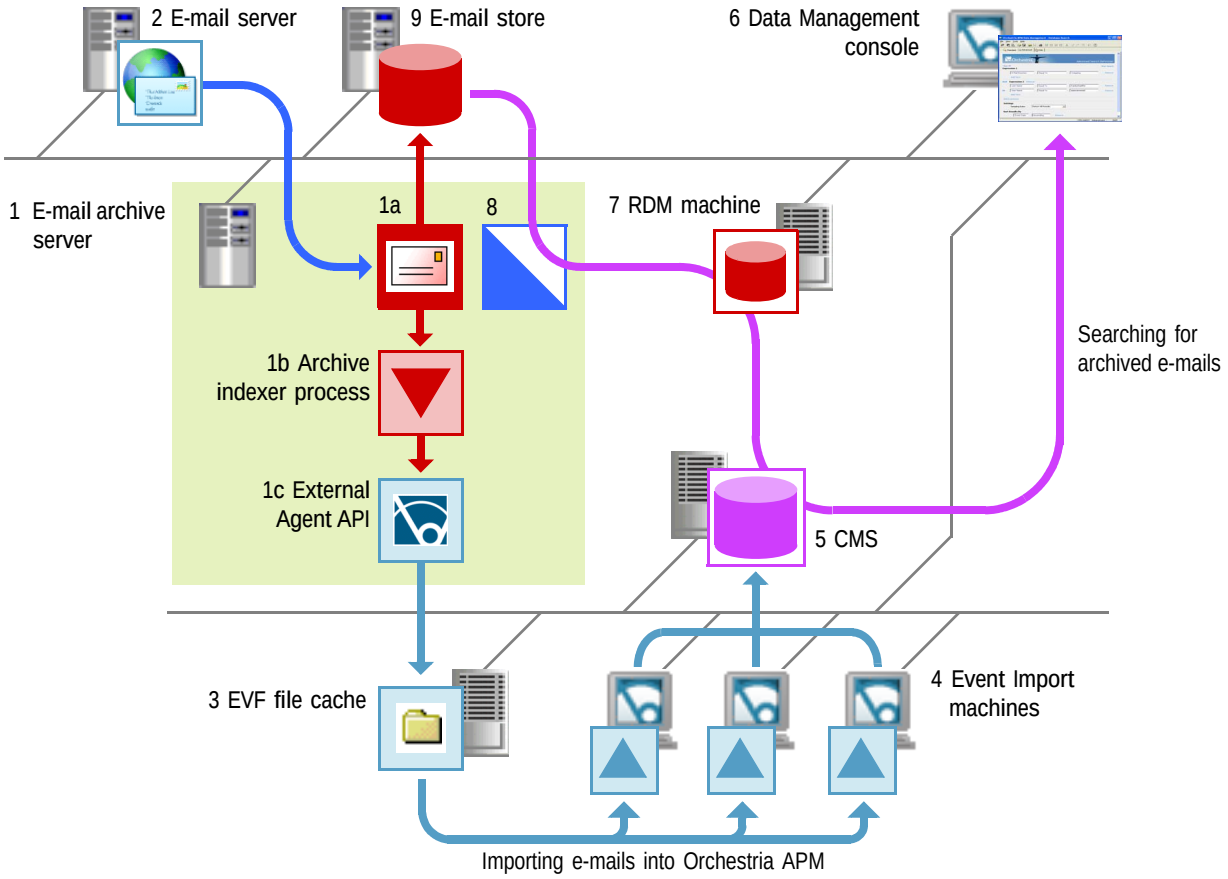
Example multi node FAST deployment

1 CMS. 2 The Orchestria APM content indexer copies captured and imported events from the CMS and submits them to the FAST system. 3 FAST admin node. This node hosts the Orchestria APM content proxy server (3a) and the following FAST services (3b): Administrative Services, the Content Distribution Service and the Query Results Processing Service. 4 Orchestria APM Data Management console submits content searches. 5 FAST search and indexing nodes. For optimum utilization of available CPU capacity, the Document Processing Service also runs on this node.

Integration with e-mail archives

The Event Import utility enables Orchestria APM to integrate with e-mail archiving solutions, importing archived e-mails into your CMS. The diagram below shows an example integration with the Zantaz EAS archive solution. This simplified diagram shows a single e-mail archive server, feeding data into a single EVF file cache. In practice, a large organization may have many servers feeding data into multiple caches.

Orchestria APM can also integrate with Symantec Enterprise Vault and Iron Mountain archives.



Orchestria APM integration with e-mail archive

1 This server hosts the e-mail archive solution, Zantaz EAS (1a). This connects to an e-mail server such as Microsoft Exchange (2) and archives messages in the e-mail store (9).

In this example, the archive solution uses an indexer process to pass data to the External Agent API (1c).

The External Agent API extracts archived e-mails and saves them as EVF files in a cache (3). This cache provides the source data for the Orchestria APM Event Import utility (4). For very large e-mail archives, you may need to run multiple Event Import utilities simultaneously to avoid import bottlenecks.

Each Event Import utility imports archived e-mails into the CMS (5). The actual message data is not saved on the CMS; instead, an identifier in the CMS database for each imported e-mail references the associated e-mail in the archive's e-mail store (9).

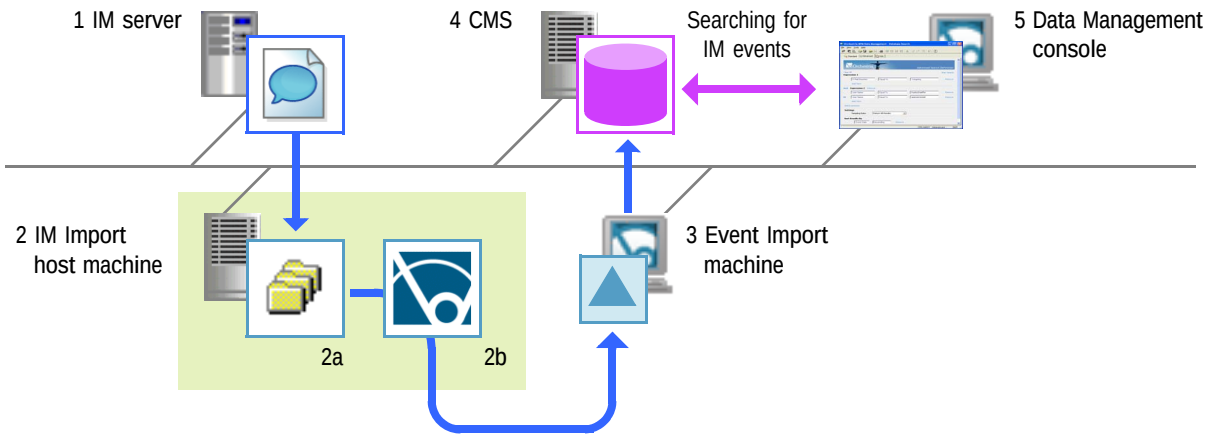
When displaying captured e-mails in the iConsole or Data Management console (6), the Remote Data Manager (7) retrieves data for e-mails archived in the e-mail store (9). In the case of Zantaz EAS, these data requests are sent via Microsoft IIS (Internet Information Services) (8).

Importing IM conversations

Orchestria APM can extract archived IM conversations and import them into a CMS. The first component in the process is IM Import. This Orchestria APM utility extracts IM conversations from log or dump files, as Orchestria APM cannot capture IM conversations directly. It then saves these extracted IM conversations to CNV files that can be accessed by the Event Import utility.

A range of parameters are available to configure your import operations; these parameters determine how IM Import generates CNV files. Event Import then uses its own parameters to determine how to identify participants in IM conversations who are internal to your organization and how to segment individual CNV files into 'chapters' (a chapter corresponds to a single Orchestria APM event. Chapterization allows for faster search and retrieval of IM events).

The diagram below summarizes the key components and processes involved when integrating Orchestria APM with an IM conversation archive solution.



Importing IM events into Orchestria APM

Importing archived IM conversations into Orchestria APM

1 IM Servers: This server hosts the instant messaging service. IM conversations are archived to the dump file source folders (2a) on the machine hosting the IM Import utility (2b).

2 IM Import host machine: IM Import itself (IMFrontEnd.exe) then extracts IM conversations from the dump files and saves them as CNV files. Currently, IM Import can extract data from these archive file formats: Instant Bloomberg, IB Inet, IB Bloomberg, IB Unified and MindAlign.

3 Event Import: This Orchestria APM utility imports these CNV files into the CMS.

4 CMS: Imported IM conversations can be searched for and reviewed in the Data Management console (5).

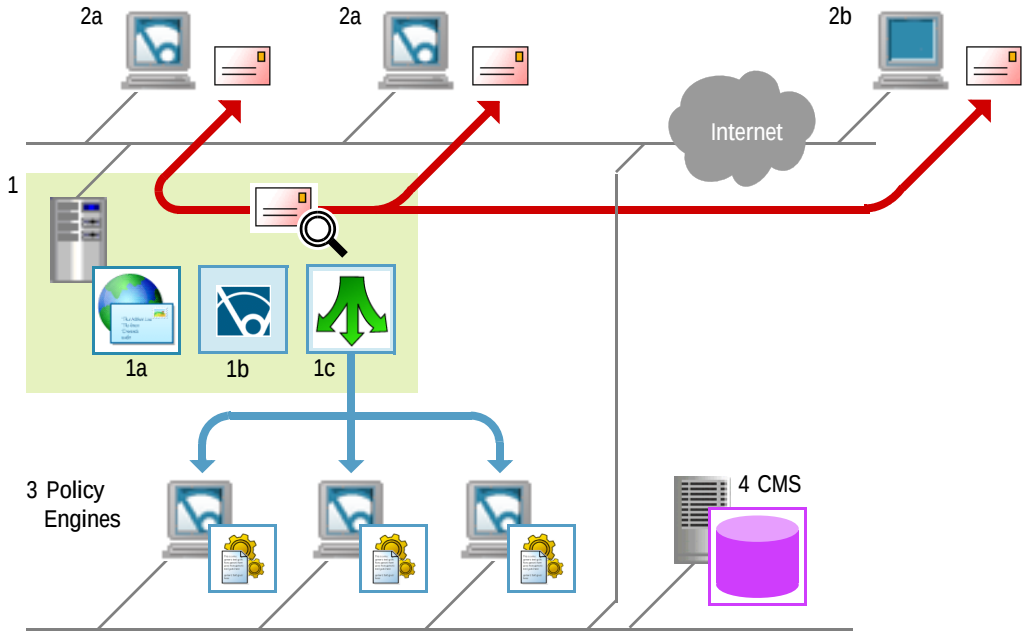
Policy engines

Policy engines permit Orchestria APM to integrate with an external e-mail event source, primarily Microsoft Exchange Server and Lotus Domino, monitoring e-mails and applying policy triggers where necessary. This contrasts with the standard Orchestria APM e-mail integration where e-mails are monitored and policy triggers applied on the client machine.

Policy engines also underlie the Import Policy feature, which provides a mechanism for connecting Event Import to policy engines, applying policy triggers to imported e-mails directly before they are stored in the CMS.

E-mails are allocated to individual policy engines by the policy engine hub. The hub and policy engines are designed to handle each e-mail with minimal delay. In particular, the hub distributes processing across multiple policy machines in a manner that achieves optimum load-balancing and maximizes throughput. It can also handle hardware failures on remote policy engine machines seamlessly, redistributing events to other policy engines if necessary.

The diagram below shows how Orchestria APM uses policy engines to integrate with Exchange Server or Lotus Domino.



Policy engines and e-mail server integration

This example shows how policy engines can be used to integrate Orchestria APM with an e-mail server.

1 E-mail server. Orchestria APM can integrate with Microsoft Exchange or Lotus Domino (1a). This server also hosts the Orchestria APM Exchange server agent or Domino server agent (1b) and policy engine hub (1c).

2 E-mail interception. E-mails transiting through the server, whether sent from internal machines (2a) or external machines (2b), are detected by the e-mail server agent and passed to the policy engine hub.

3 Policy engines. The hub (1c) creates connections between the e-mail server agent and each policy engine and maintains performance and event processing statistics for each policy engine host machine.

When hub receives a new e-mail from the e-mail server agent, it allocates the e-mail to the least heavily loaded policy engine (that is, the policy engine that can process the new e-mail most quickly). The policy engine then analyzes the e-mail and applies policy triggers as necessary.

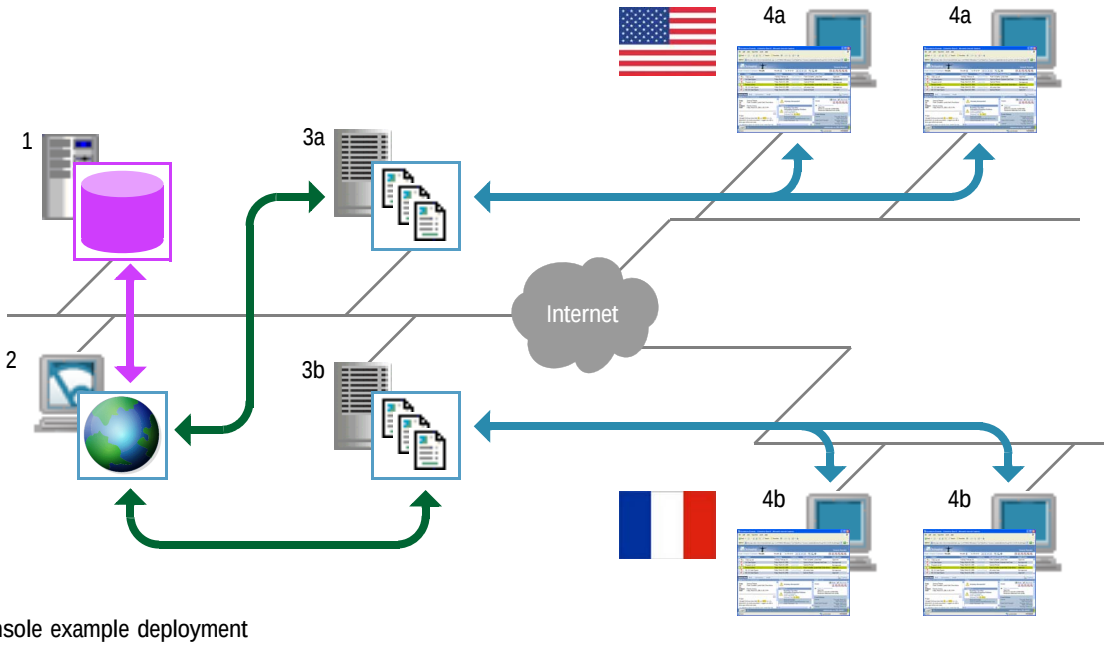
4 CMS. All resulting e-mail events are replicated up to the CMS.

iConsole

The iConsole delivers much simplified deployment and upgrade procedures and a significant reduction in maintenance and support overheads. It also minimizes the impact on network bandwidth and allows end-users to access a CMS over the Internet (for example, by using a virtual private network).

To deploy the iConsole, you must install a front-end Web server and application server. These are provided as separate components to allow maximum flexibility when deploying the iConsole. The front-end Web server generates the HTML content for the iConsole screens and also submits any event searches to the application server. iConsole users direct their browsers to a URL that identifies the machine hosting the front-end Web server. The application server provides the Web service that connects to the CMS. It enables all event search and auditing activity conducted in the iConsole to be written to the CMS.

Each front-end Web server can only connect to a single, specific application server, but it is possible to connect multiple front-end Web servers to a single application server. You can also have multiple application servers, each serving different front-end Web servers but all connected to the same CMS. Larger organizations may choose this configuration for load-sharing purposes.



iConsole example deployment

1 CMS. This services all search requests submitted by the application server. All search SPs are stored in the CMS database; all XML search definition files are stored in the CMS file system.

2 iConsole application server. This submits iConsole event searches and audit updates to the CMS and returns search results to the front-end web server. Each application server is parented to a single CMS. If required, multiple application servers can connect to a single CMS.

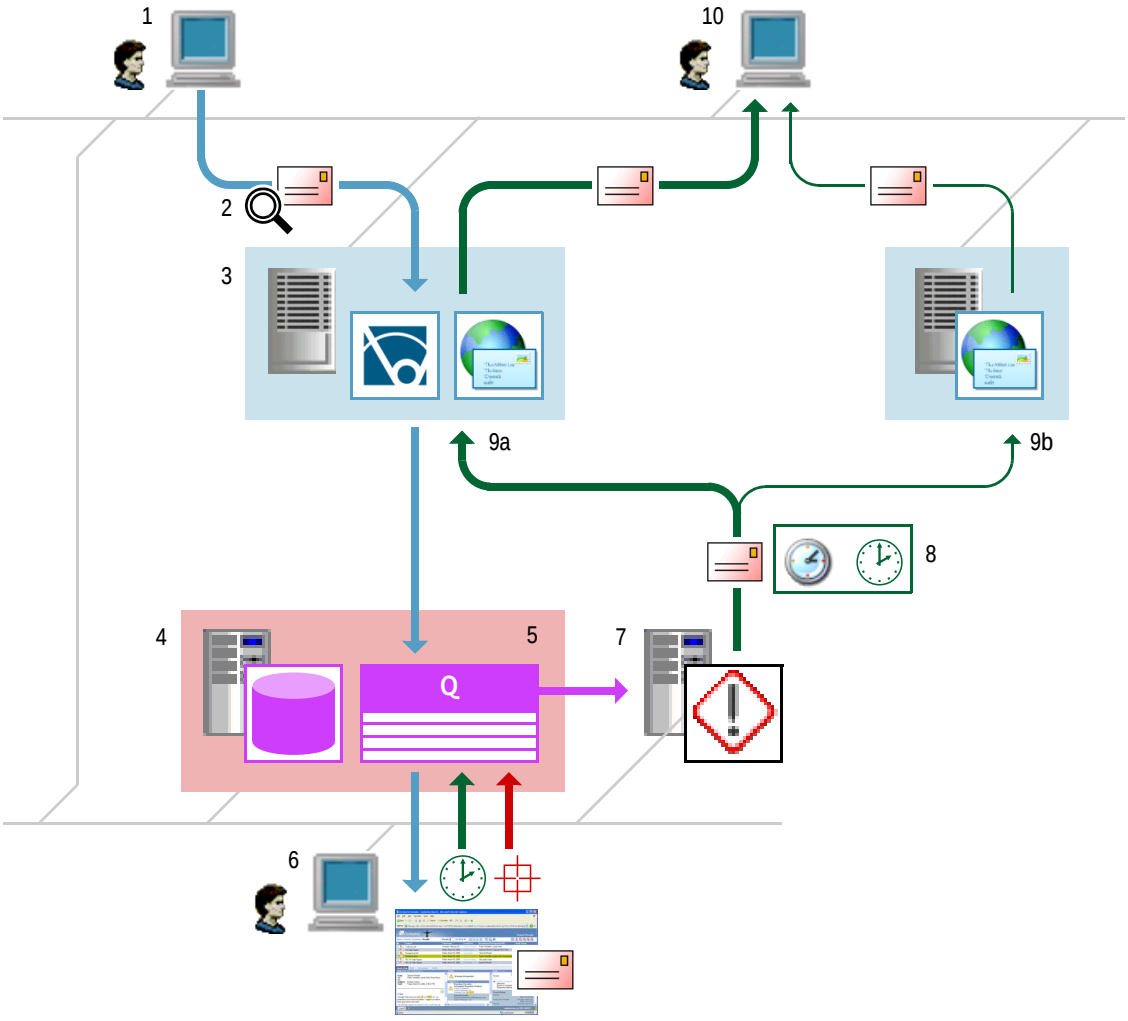
3a, 3b iConsole front-end Web servers. These generate the HTML content for the various screens in the iConsole. In this example, two front-end Web servers each serve separate groups of iConsole users (for example users based in New York and Paris), but connect to a single shared application server.

4a, 4b Browser-based iConsoles. Reviewers and administrators use the iConsole to search for and retrieve events stored on the CMS and to update audit details for these events. The iConsole URL incorporates the name or address of the front-end Web server host. In this example, the New York iConsoles (4a) connect to front-end Web server 3a, while the Paris iConsoles (4b) connect to front-end Web server 3b.

Quarantine Manager

SEC regulatory requirement 472 requires that certain categories of documents sent to multiple external recipients must be approved by an appropriate representative. The Orchestria APM quarantine feature enables organizations to enforce this requirement.

The Quarantine Manager ensures that e-mails released from quarantine are sent on to their original recipients. To achieve this, it regularly queries the CMS for released or timed-out e-mails and forwards these to their intended recipients.



Quarantine procedure: Example based on Exchange server integration

This example shows how the Quarantine feature operates in conjunction with Exchange server integration. However, it can also operate in conjunction with Outlook client agents.

An e-mail is sent (1) and monitored by Orchestria APM (2) as it transits through the Exchange server (3). A control trigger quarantines the e-mail. The CMS (4) maintains a queue of quarantined e-mails (5). A reviewer (6) checks quarantined e-mails in the iConsole or Data Management console. The reviewer can either release or reject a quarantined e-mail.

The Quarantine Manager (7) regularly checks the quarantine queue on the CMS, checking for e-mails that have been released or which have timed out (8). It then forwards these e-mails, either via the original Exchange server (9a) or, if so configured, though an alternative Exchange server (9b) to the intended recipient (10).

For simplicity, this diagram omits the policy engine hub and policy engines.

chapter 2

Deployment tasks

This chapter outlines the key tasks when deploying Orchestria APM. Such deployments can be very complex, and vary from one organization to the next. This chapter attempts to map a route through the overall deployment process, plotting each major task, and then breaking each major task down into a series of installation or configuration steps. Where necessary, individual steps include a cross-reference to sources of further information.

The start point is the flow chart on page 14. Each deployment begins with two compulsory steps: Setting up an Orchestria APM database and installing a CMS. Thereafter, the deployment sequence varies according to which Orchestria APM features your organization intends to use. For example, if your reviewers will be running content searches, you need to install the Orchestria APM Content Services. Likewise, if you intend to integrate Orchestria APM with Exchange Server or Lotus Domino, you need to install policy engines and then the Exchange or Domino server agent and policy engine hub. If you intend to deploy Orchestria APM client agents on your users' workstations, you will need to deploy gateways and client machines.

Essential reading

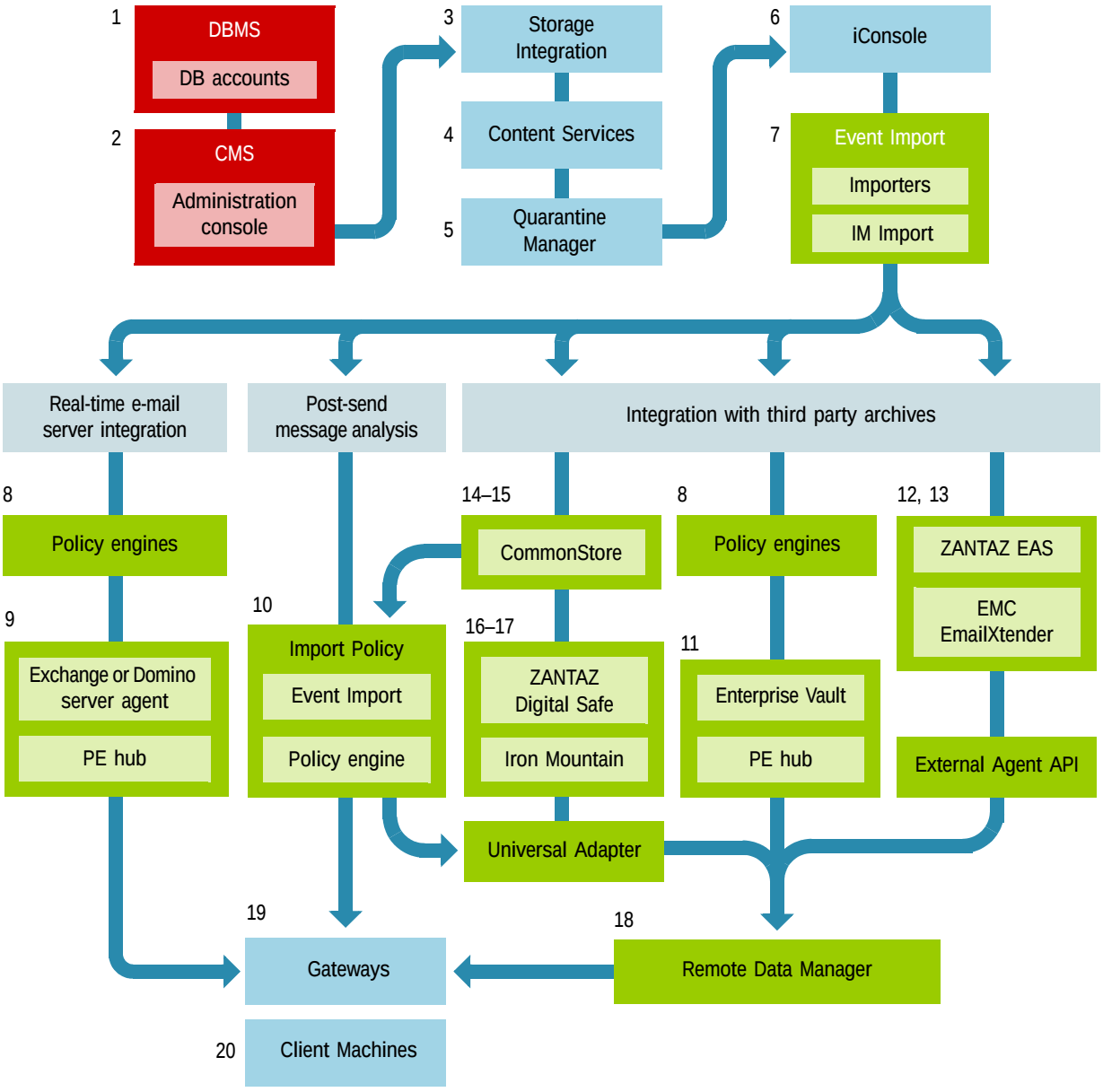
The following sections contain numerous references to further sources of information. In particular, when you begin your Orchestria APM deployment, the following documents provide essential instructions or reference information:

- **Database guide:** Provides guidelines on configuring Oracle and Microsoft SQL Server databases.
- **Deployment guide:** Provides instructions for installing and configuring key Orchestria APM features and components, including the CMS and gateways; Account Import; Event Import; policy engines, hubs, and the Exchange and Domino server agents; Import Policy; Content Services; integration with third party archive and storage solutions; and the Quarantine Manager. It also describes how captured or imported e-mail addresses are mapped to Orchestria APM user accounts.
- **Administrator guide:** Provides instructions for all console operations, including: managing Orchestria APM user and machine accounts; editing policies to capture and control user e-mail and Web behavior; retrieving and auditing e-mail and Web events.

These guides are available in the \Software\Docs folder on your Orchestria APM distribution media.

Orchestria APM deployment tasks

The major tasks in an Orchestria APM deployment are summarized below in the flow chart below. Only tasks **1** and **2** (configuring a database and setting up the CMS) are compulsory. The remaining tasks are optional and the actual deployment path varies from company to company, depending on operational requirements. Details about each major task are given on pages 16 to 41.



Key: Flow chart items are summarized on page 15.

Deployment tasks: Flow chart key

1 **Database:** Set up your Orchestria APM database engine (Oracle or SQL Server) and, optionally, your database accounts. See page 16.

2 **CMS:** Install and configure your CMS> then set up your machine policies and the default user group policy. See page 17.

3 **Storage integration:** Configure the CMS for integration with a third-party storage solution such as EMC Centera or IBM DB2 Content Manager. See page 20.

4 **Content Services:** Install a content database, then index documents into it. See page 21.

5 **Quarantine Manager:** Install a Quarantine Manager and mark e-mails for quarantine. See page 23.

6 **iConsole:** Install and configure the application server and front-end Web server. See page 24.

7 **Event Import:** Install Event Import and configure import operations for e-mails and IM events. See page 26.

8 **Policy engines:** Install and configure individual policy engines. See page 28.

9 **Exchange or Domino integration:** Install and configure the server agent and a policy engine hub. See page 29.

10 **Import policy:** Install and configure Event Import and a policy engine (or optionally, multiple policy engines and a PE connector). See page 30.

11 **ZANTAZ EAS integration:** Install the External Agent API, then configure the EAS indexer process to connect to it. See page 31.

12 **Enterprise Vault integration:** Install and configure the EV server agent and a policy engine hub. See page 32.

13 **ZANTAZ Digital Safe integration:** Install and configure the Universal Adapter and the Digital Safe Adapter. See page 34.

14 **IBM DB2 CommonStore integration for Exchange:** Install and configure IBM DB2 CommonStore, Event Import and the Universal Adapter. See page 35.

15 **IBM DB2 CommonStore integration for Domino:** Install and configure IBM DB2 CommonStore and Event Import. See page 36.

16 **EMC EmailXtender integration:** Install the External Agent API, then configure the EMC EmailXtender process to connect to it. See page 37.

17 **Iron Mountain integration:** Install and configure the Universal Adapter and the Iron Mountain Adapter. See page 38.

18 **Remote Data Manager:** Install this to allow console users to search for and retrieve events archived in remote third party archives. See page 39.

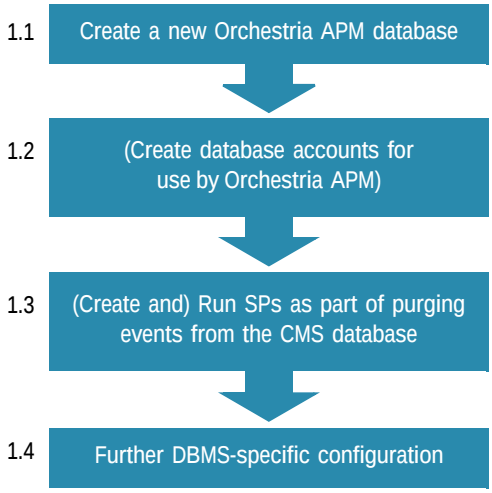
19 **Gateways:** Install gateways for resilience and load-balancing in client machine deployments. See page 40.

20 **Clients:** Deploy for desktop monitoring and control of users' e-mail and Web activity. See page 41.

1 Database configuration

Before installing the CMS (or a gateway server), your chosen database engine must already be installed and correctly configured. Orchestria APM supports two database engines, Microsoft SQL Server and Oracle.

For full database configuration and optimization guidelines, see the Database guide; find this guide in the \Software\Docs folder on your Orchestria APM distribution media. The basic configuration steps are:



Database configuration

These steps are described below.

1.1 Create a new database for Orchestria APM.

1.2 Orchestria APM uses various database accounts to access the CMS database—see the next section. You can create these accounts automatically when you run the CMS installation wizard. Alternatively, you may prefer to create them manually before deploying the CMS. Instructions are provided in the Database guide; search the index for 'primary user' and 'schema owner'.

1.3 When purging events from the CMS database, the Orchestria APM infrastructure invokes stored procedures (SPs). Orchestria APM provides various public purge SPs, or you can design your own custom purge SPs, including SPs to run immediately before or after a purge.

1.4 Perform further configuration specific to your chosen DBMS. For example, if using Oracle you need to configure the listener and set the initialization parameter.

Database users for Orchestria APM

Orchestria APM needs two database accounts that it can use to access the CMS database. These are the Primary User and Search User. For Oracle If required, you can also specify third Oracle account, the Schema Owner. These users are summarized below.

- **Primary User:** This is the main Orchestria APM database account. The infrastructure uses this account to access the CMS database. By default, this user also 'owns' the database schema unless a Schema Owner is specified (see below).

  If a separate schema user is specified, the primary user is also sometimes known as the 'shadow user'.

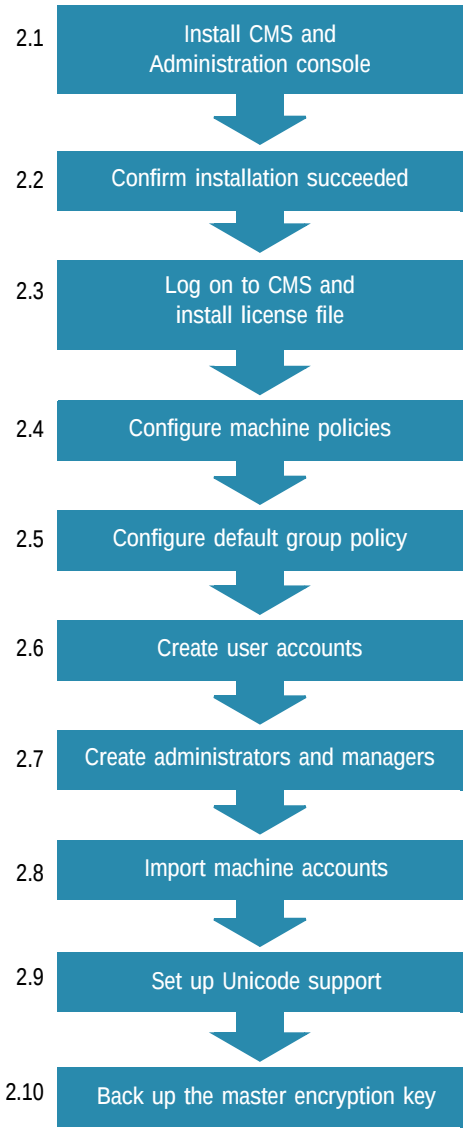
- **Search User:** All Orchestria APM consoles use this account when searching the CMS database for events. This is a secure account that is subject to 'row level security'. This ensures that reviewers cannot see events associated with users outside of their management groups.

  'Row level security' is a reference to event records in the relevant database tables.

- **Schema Owner:** For Oracle databases only. This optional account owns the database schema. Some organizations choose to have separate accounts for the primary user and the database owner. This is typically for security reasons, for example, to ensure that employees cannot connect to the CMS database as the primary user and delete sensitive data or drop the underlying database objects.

2 CMS installation and configuration

Installing and configuring your CMS involves several steps. These are summarized below and described in more detail on the following pages:



CMS installation and configuration

These steps are described on the following pages.

Unattended installations

Note that you can also configure an unattended installation using command line options for msiexec.exe, the Microsoft Windows Installer service. Orchestria APM supports a range of variables that you can use as msiexec.exe parameters. For details, see the Deployment guide; search the index for 'unattended installations'.

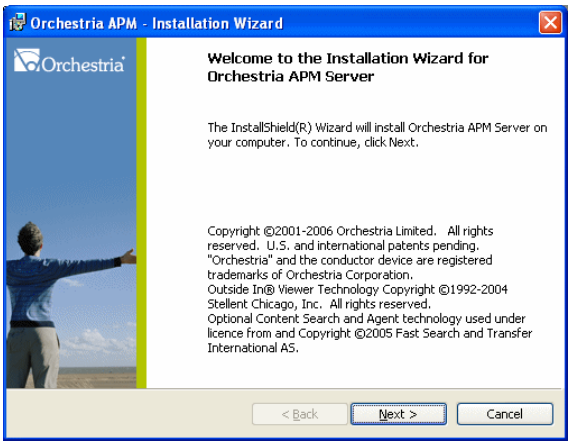
Installation procedure

2.1 Install the CMS

Use the Orchestria APM server installation wizard. Note that you will need to install at least one Administration console for steps **2.3** through **2.8**.

In the Administrator Credentials screen, you must supply a name and password for the Primary Administrator account. Remember these credentials—to configure Orchestria APM, you will need to log on to the CMS using this account (step **2.3**).

For installation instructions, see the Deployment guide; search the index for 'CMS: Linux, Solaris or Windows: installing'.



Orchestria APM server installation wizard

2.2 Confirm that the CMS installed successfully

In the Windows Services applet, confirm that the Orchestria APM infrastructure service has started.

If the installation failed, check the Orchestria APM 'Activity' and 'System' logfiles for any error messages. These are the activity*.log and stderr*.log files in Orchestria's \data\log subfolder of the Windows All Users profile; see the Administrator guide; search the index for 'logfiles'. For further details, see the Administration console online help; search the index for 'logfiles'.

2.3 Log on to the CMS and install your license file

The following steps require that you use the Administration console. To do this, you must log on to the CMS as the Primary Administrator (step **2.1**). This ensures that you have adequate administrative privileges and management group coverage to configure your Orchestria APM installation.

At this stage, we also recommend that you install your license file. This unlocks the Orchestria APM policy modules available to your organization. For details about obtaining and installing a license file, see the Deployment guide; search the index for 'license files'.

2.4 Configure and back up the machine policies

Next, you need to configure the CMS machine policy and (if you plan to deploy gateways and client machines) the common gateway and common client policies. In particular, you must set up:

- **Event purging:** You must turn on event purging to prevent free disk space falling to dangerously low levels. This particularly applies to the common gateway and common client policies.
- **Free disk space monitoring:** These settings determine how low free disk space can fall on Orchestria APM machines before the infrastructure is suspended. By default, these settings are optimized for client machines so you need to adjust these values in your CMS policy and common gateway policy.
- **Common gateway and client policies:** In addition to database purging and free disk space monitoring, you will probably want to amend other policy areas such as encryption and replication.
- **Handling for new user accounts:** If required, you can edit the CMS policy to support self-enrolment. That is, it automatically creates new accounts when an unrecognized user uses their e-mail application or browser after installing Orchestria APM client agents. If you do this, you must also configure the 'default group' policy (see step **2.5**).

For details about which settings to edit, see the Deployment guide; search the index for 'machine policy: configuring: CMS'.

For backup purposes, we recommend that you export these newly configured policies. Orchestria APM provides polimex.exe and wgnpol.exe for exporting and importing policies to and from files. Find these utilities in the \Software\Win32\Support folder on your Orchestria APM distribution media. For usage instructions, see wgnpol.htm in this folder.

2.5 Configure the 'default group' user policy

If you configure Orchestria APM to automatically create new user accounts, you must ensure that the policy for the default group is correctly configured. This is because these users are automatically assigned to the default group. In particular, these policy areas need to be correctly specified:

- **Internal e-mail addresses:** Orchestria APM flags outgoing e-mails as internal when all recipient addresses match an 'internal address pattern'. It flags incoming e-mails as internal if the sender's address matches an internal address pattern. Internal address patterns are defined by the Internal E-Mails setting in the user policy. This is in the System Settings\Definitions policy folder.
- **General e-mail handling:** Other settings in the System Settings policy folder determine, for example, how Orchestria APM handles e-mails addressed to distribution lists and whether it stores

the message class of captured e-mails. For details, see the Administrator guide; search the index for 'System Settings'.

▸ **Capture and control triggers:** These triggers provide enormous flexibility to restrict or guide users' e-mail and Web activity across your organization. For example, you can block inappropriate e-mails. You can also warn or notify users if, say, an e-mail requires their attention. You can even forward intercepted e-mails to other accounts. You need to define the conditions that activate a trigger. For details, see the Administrator guide; search the index for 'triggers'.

2.6 Create your hierarchy of users

Now create or import the accounts for individual Orchestria APM users and organize these accounts into user groups. Remember to define appropriate group policies for your new user groups (see step **2.5** for key policy considerations). For details, see the Administrator guide; search the index for 'users: adding' and 'groups: editing policies'.

To simplify mass deployments, Account Import can import user accounts into the Administration console, either from an external data source such as an LDAP directory. See the Deployment guide; search the index for 'Account Import'. An example LDAP import operation is shown on page 19.

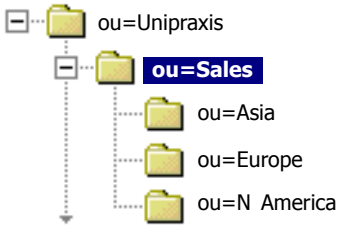
2.7 Create your administrators and managers

You can promote ordinary users into administrators or managers by granting them administrative privileges. You can limit the scope of their administrative authority by withholding specific privileges and controlling which groups they can manage. For details, see the Administrator guide; search the index for 'administrators: creating'.

You will also need to install Administration consoles for your Orchestria APM administrators. You can do this when you deploy gateways and client machines see (tasks 19 and 20 on pages 40 to 41). Alternatively, you can perform a console-only installation. See the Deployment guide; search the index for 'consoles: console-only installations'.

Example LDAP user import operation

1 The source LDAP directory is 'ou=Sales'.

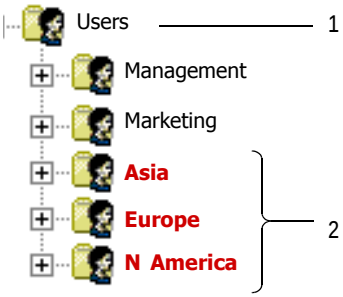


Example LDAP directory structure

2 The target Orchestria APM parent group is 'Users'.

Orchestria APM user hierarchy: Before importing

3 The following changes are imported to the Orchestria APM user hierarchy:



Orchestria APM user hierarchy: After importing

1 Parent group. LDAP users imported into this group.
2 Imported groups. The original LDAP directory structure is preserved in the Orchestria APM user hierarchy.

2.8 Import machine accounts

To simplify mass deployments, you can optionally bulk create new machine accounts and pre-assign client machines to parent servers in advance of the Orchestria APM rollout. This enables you to deploy multiple client machines using a single source image (which identifies a single parent server) while ensuring that each client machine automatically connects to its 'correct' parent server immediately after installation. See the Deployment guide; search the index for 'Account Import: machines'.

2.9 Support for Unicode characters

All Orchestria APM consoles now support Unicode character sets. To implement Unicode support on Oracle CMSs, you need to set up the database for Orchestria APM to use UTF-8 encoding for the DBMS code page. For full details, see the Deployment guide; search the index for 'Unicode characters: general configuration'.

2.10 Back up the master encryption key

The CMS uses a password-protected key to provide highly secure data management. If you need to restore the CMS, you will need to restore the key. For this purpose, Orchestria APM provides a data management utility (wgnmgmt.exe) for exporting and re-importing these keys. When you export the key, it is written to a password-protected file. *Keep this file in a secure location, for example, on a floppy disk in a fire-proof safe!*

For full details, see the Deployment guide; search the index for 'master encryption key'.

3 Storage integration

Orchestria APM can integrate with the following third party object storage solutions:

- EMC Corporation's Centera content addressed storage (CAS) solution
- IBM DB2 Content Manager
- NetApp SnapLock

These ensure long-term content integrity and online access for large volumes of fixed data. Integration between Orchestria APM and these systems provides your enterprise with an end-to-end solution to your e-mail and Web risk management and storage needs.

We recommend that you set up EMC Centera, IBM DB2 or NetApp SnapLock integration as soon as possible after deploying Orchestria APM. See the Deployment guide; search the index for 'Centera integration', 'IBM DB2 Content Manager integration' or 'NetApp SnapLock integration'.

4 Content Services

Orchestria APM Content Services provide access to the Content Search and Content Agent features. Based on innovative pattern-matching technology and intelligence contained in your Orchestria APM Content database, these features give you the ability to capture, control, or search for Web and e-mail documents based on their text content. Full details about these features are given in the Administrator guide; search the index for 'content search' or 'content agents'.

Software components

Content Services comprise the following components:

- **Content proxy server:** This enables Orchestria APM consoles to access a content database when running a content search for captured events and training content agents. Each content proxy server is tied to a single parent CMS. Multiple proxy servers can share a parent CMS.
- **Content agent builder:** This enables Orchestria APM to train a content agent to detect specific categories of Web or e-mail documents based on their text content.

  *If your organization intends to train content agents, you **must** install the content proxy support component on a FAST host machine.*
- **Content indexer:** This enables you to extract captured data from your CMS for indexing into a Content database. This utility includes the Orchestria APM Content Indexer service, which can monitor your CMS for newly captured data and index specified data into your content database.
- **Content database:** This is the term used by Orchestria to describe the engine or system into which you can index captured data. You use the Content Search feature to retrieve captured e-mail and Web documents stored in the content database.

  For FAST-based content services, the content database equates to the search index, typically distributed across multiple 'search and indexing' nodes.
- **Content Purge:** This enables Orchestria APM to delete content from the FAST database. You can install this utility on any machine in your Orchestria APM enterprise.

Deploying Content Services

Installing Content Services involves the following steps.

Briefly, for a FAST-based deployment you must first install the 'admin' and 'search and indexing nodes'. Then install the subsystem components that enable Orchestria APM to communicate with the content database. To complete the installation, you must then install the components that interact with the Orchestria APM infrastructure. Finally, you need to confirm that the components installed and registered successfully. You can then populate the content database with indexed documents. Further details on each step are provided below.

For full installation guidelines and instructions, see the Deployment guide; search the index for 'content services'. Various technical notes are also available, covering content database backups and the installation of multiple content databases on a single host; please contact the service desk for details (see page 5).

4.1 Install the FAST nodes

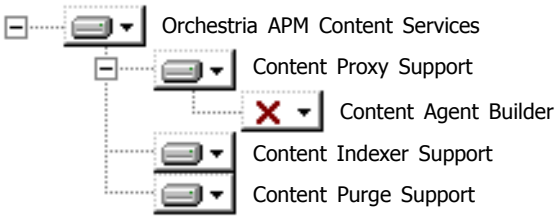
For a FAST-based deployment, you must first separately install and configure the various 'nodes' or host machines that collectively comprise the content database. You typically require a single 'admin node' and multiple 'search and indexing nodes'. The installation is a two-step process: First, you must run the FAST setup program to configure generic FAST host machines. Then you run an Orchestria APM script to customize the FAST configuration.

4.2 Install the subsystem components to enable communication with the content database

Next, you must install the subsystem components for the content proxy server and content indexer that enable Orchestria APM to communicate with the content database. These components are available through the Orchestria APM Content Services installation wizard.

Run this wizard on any machine; it does not have to be an existing Orchestria APM machine.

For FAST-based deployments, choose the features you want to install in the Custom Setup screen. Then, in the Content Database Configuration screen, specify the name or IP address of the admin node machine and the base port number you specified when configuring your FAST hosts in step **4.1**.



Custom Setup screen: FAST Content Services

*If your organization intends to train content agents, you **must** install the content proxy support component on a FAST host machine.*

4.3 Install the components that interact with the Orchestria APM infrastructure

We recommend that you follow this step last, after installing the subsystems and, for FAST deployments, the FAST host machines. This is to ensure that the necessary Orchestria APM services start automatically after installation.

For FAST-based deployments, you must now install the content proxy server and content indexer components that interact with the Orchestria APM infrastructure. These components are available through the Orchestria APM server installation wizard.

For FAST-based content services, install these components on the same host machine as the corresponding subsystem components. Likewise, you must install the Content proxy Server on the same machine as the Content Proxy Support component. The exception to this rule is the Content Indexer Console; you can install this on any machine.

4.4 Confirm the components installed successfully

In the Windows Services applet, confirm that these services have started:

- Orchestria APM Content Indexer
- Orchestria APM Content Proxy Server

If the installation failed or a service failed to start, check the Orchestria APM logfiles for any error messages. These are the index*.log files in Orchestria's \data\log subfolder of the Windows All Users profile; see the Administrator guide; search the index for 'logfiles'.

4.5 Confirm the proxy server registered successfully

If you install a content proxy server, you need to confirm that proxy server has correctly registered with the CMS. To do this, open an Administration console:

- **Either** choose Tools > Options and go to the Content Proxy tab. If the Content Proxy Server has correctly registered with the CMS, its host machine will be listed in the drop-down list of servers.
- **Or** expand the My Servers list and select the parent CMS. The Server Machine screen lists all utility services parented to this CMS. The Content Proxy Server will be listed here.

4.6 Populate the content database with indexed documents

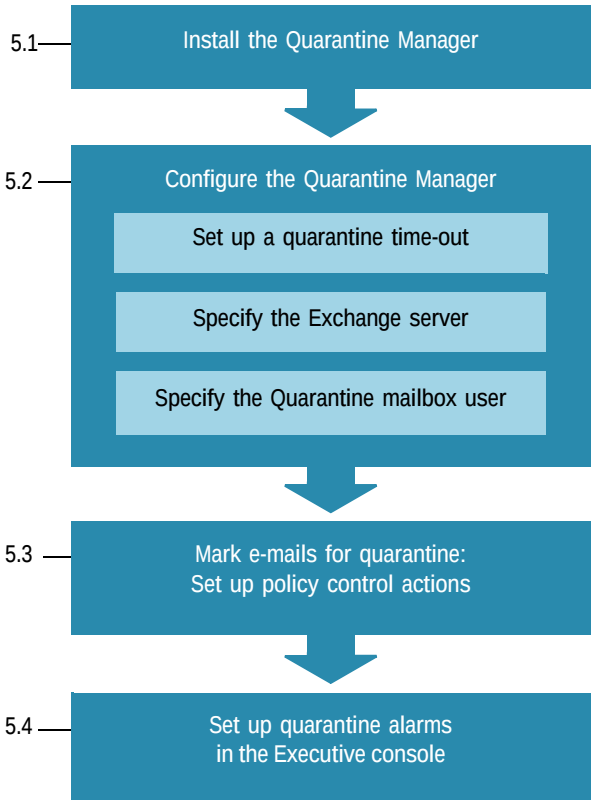
Even if there are not yet any events saved in the CMS database, you can still configure an indexing job now to continuously monitor the CMS and index new events as they are captured or imported.

To do this, start the content indexer and configure a 'notification' indexing job. As soon as events are saved to the CMS, they will be indexed into the content database. For full usage instructions, please refer to the content Indexer online help.

5 Quarantine Manager

Setting up Orchestria APM to quarantine e-mails that require an urgent review is a four-step procedure, summarized below.

For full details, see the Deployment guide; search the index for 'Quarantine Manager'.



Quarantine events: Deployment procedure
These steps are described opposite.

5.1 Install the Quarantine Manager

You install the Quarantine Manager using the Orchestria APM server installation wizard. We recommend that you install the Quarantine Manager on a utility machine.

5.2 Configure the Quarantine Manager

After installation, you must configure how the Quarantine Manager handles quarantined e-mails. To do this, you must edit the registry on the Quarantine Manager host machine. briefly, you must:

- Set up a quarantine time-out to automatically release unreviewed e-mails from quarantine after a specified period.
- Specify which Exchange server the Quarantine Manager connects to when forwarding released e-mails.
- Specify the user account used by the Quarantine Manager when forwarding released e-mails.

5.3 Mark e-mails for Quarantine

Now you need to set up the Quarantine feature to identify e-mails that need urgent reviewing. To do this, edit control triggers and actions in the user policy. For details, see the Administrator guide; search the index for 'quarantined e-mails'.

5.4 Set up a Quarantine alarm

Use the Executive Console to set up an alarm to alert reviewers when new e-mails are added to the quarantine list. For details, see the Administrator guide; search the index for 'quarantined e-mails'.

6 iConsole deployment

To deploy the iConsole, you must install a front-end Web server and application server. These are provided as separate components to allow maximum flexibility when deploying the iConsole. For example, you may prefer to install the front-end Web server on your existing corporate Web server while installing the application server on an existing Orchestria APM server.

Also, each front-end Web server can only connect to a single, specific application server, but you can connect multiple front-end Web servers to a single application server. This configuration may be preferable if your iConsole users are based in various offices around the world because it enables each user to connect to a local front-end Web server, with each front-end Web server connected to a central application server.

You can also have multiple application servers, each serving different front-end Web servers but all connected to the same CMS. Larger organizations may choose this configuration for load-sharing purposes.

An iConsole deployment requires the following steps. For full details, see the Deployment guide; search the index for 'iConsole: requirements'.

Installation

6.1 Prepare the host machines

When installing an iConsole application server, the host machine must already have an Orchestria APM server installed. If this not the case, install a server now. We recommend installing the application server on an Orchestria APM utility machine.

For both the Application server and Front-end Web server, the host machine must also be running Microsoft Internet Information Services (IIS) version 5 or higher and .Net Framework version 1.1 SP1, or higher.

6.2 Set up SMTP e-mail

To allow iConsole users to send audit e-mails, you must configure the front-end Web server so it can connect to an SMTP server (that is, a machine that can deliver SMTP e-mails).

6.3 Install the Application server and the Front-end Web server

To do this, run the iConsole installation wizard. If you are installing the Application server and Front-end Web server on separate machines, you must specify which application server it connects to.

6.4 Perform various post-installation tasks

After installing the iConsole, there are various optional post-deployment tasks. These include:

- **Install the default event searches:** To make the default searches available to your iConsole users, you must load the default stored procedures (SPs) into the CMS database, then load and publish the XML search definitions.
- **Allow iConsole users to connect to multiple CMSs:** You can edit registry value on the application server host machine to allow iConsole users to connect to multiple CMSs.
- **Reconfigure the session timeout:** By default, iConsole sessions terminate automatically. To change the default timeout, you edit the registry on the front-end Web server host machine.
- **Rename the front-end Web server virtual directory:** This virtual directory is incorporated into the target URL for iConsole users. If required, you can rename it.
- **Specify the security account for the virtual directory:** For Windows Server 2003 machines only. If the virtual directory for the front-end Web server uses a non-default security account, you need to specify this account in IIS.
- **Enable anonymous access:** This is needed if the application server and front-end Web servers cannot communicate using Windows authentication.
- **Configure the search results cache:** You can specify the maximum number of search results and the retention period for these results.

- **Set up event auditing:** To enable your reviewers to audit events using the iConsole, you need to manually set up this feature in the Administration console by choosing Tools > Options and selecting Yes on the message that is displayed.

- **Define a global sender for audit e-mails:** These are e-mails sent by reviewers to colleagues. You can configure the From: field so it is always set to the same sender, for example, 'Unipraxis Compliance Team' or 'compliance@unipraxis.com'.

6.5 Start the iConsole

Users simply browse to a specified URL to start using the iConsole. If Single Sign-on is enabled on the CMS (see below), they will not need to log on, but can begin searching for events immediately. The iConsole URL is:

```
http://<FE_Server>/<virtual dir>
```

Where: `<FE_Server>` is the name or IP address of the host machine for the front-end Web server and `<virtual dir>` is the virtual directory for the front-end Web server. For example, if the front-end Web server is hosted on the server UX-WebSvr-01, the iConsole URL is:

```
http://UX-WebSvr-01/orchestria
```

6.6 Define new iConsole event searches

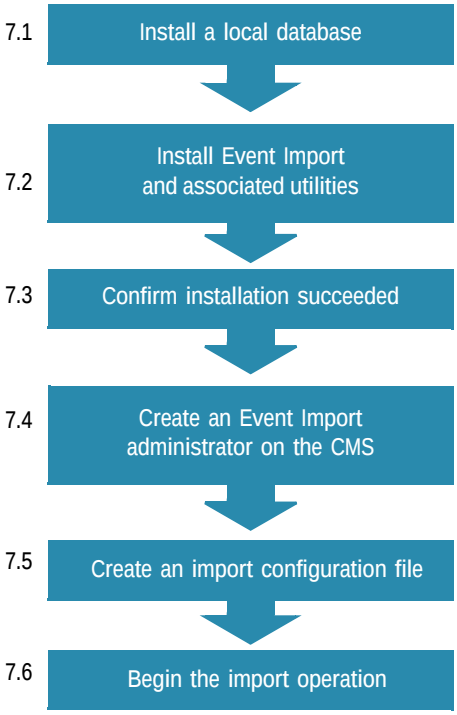
To create new event searches and make them available to all iConsole users, you must first write a stored procedure (SP) in the CMS database. This defines a specific search for captured events. You must then create and install an XML search definition file onto the CMS. This defines the search parameters and the layout of the search results screen. Finally, after testing the new search, you must publish it to make it available to all iConsole users.

For full details, including SP syntax and XML schema reference information, see the iConsole Search Definition guide.

7 Event Import

Event Import enables Orchestria APM to integrate with e-mail archiving products, extracting e-mails extracted from an archive and importing them into the CMS. Event Import can also import e-mails saved in archive files (for example, PST and MSG files) and archived IM conversations.

As part of your overall Orchestria APM deployment, an Event Import deployment involves the following steps:



Event Import installation and configuration

These steps are described on the following pages.

Deployment procedure

7.1 Install a local database

Event Import must be installed on an Orchestria APM server, which requires a local database. The installation procedure is the same as for the CMS database (see task 1 on page 16).

7.2 Install Event Import and IM Import

The basic Event Import components can be installed using the Orchestria APM server installation wizard. If you also want to archive imported IM conversations, further steps are necessary.

▶ **Event Import:** To do this, run the Orchestria APM server installation wizard. Note the logon requirements for the Event Import service if you are importing events from a shared network folder or Exchange mailbox. For installation and logon instructions, see the Deployment guide; search the index for 'Event Import utility' and 'logon requirements'.

▶ **IM Import:** Orchestria APM does not capture IM conversations directly, but it can extract archived IM conversations and import them into a CMS. The IM Import utility, IMFrontEnd.exe, extracts IM conversations from dump files and converts them into CNV files, which can then be accessed by Event Import. You configure IMFrontEnd.exe operations by specifying parameters in a configuration file. For installation and configuration instructions, see the Deployment guide; search the index for 'IM Import'.

7.3 Confirm that the installation succeeded

In the Windows Services applet, confirm that these services have started:

- **Event Import:** In the Windows Services applet, confirm that the 'Orchestria APM Event Importer' service has been created. You must manually start this service to begin your first import job.

- **IM Import:** You do not need to check that IM Import installed correctly. It is installed by simply copying a folder from the Orchestria APM distribution CD to the host machine.

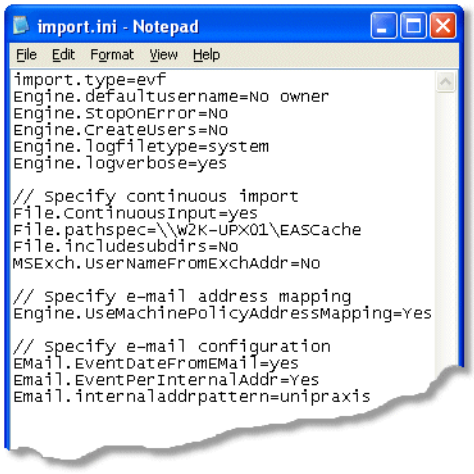
7.4 Create an Event Import administrator on the CMS

When you run Event Import, you must log on to the CMS as an Orchestria APM administrator. You do this using import parameters in the configuration file. But note the requirements for this account. Specifically, this user account must have the Events: Allow event import and Events: Allow bulk session management administrative privileges. It must also have a management group that encompasses all the users against which you are importing e-mails.

You must create this account on the CMS before running an import job. For details, see the Deployment guide; search the index for 'logon requirements for Event Import'.

7.5 Create an import configuration file

You configure import jobs by creating a configuration file, import.ini. This specifies a series of import parameters. For parameter and file format details, see the Deployment guide; search the index for 'Event Import utility: configuration file'.



Example import.ini configuration file

7.6 Begin the import operation

For continuous import operations, you must restart the Orchestria APM Event Importer service (wgnimpsv.exe). To start an individual import operation, run wgnimp.exe. For full details, see the Deployment guide; search the index for 'Event Import utility: running import operations'.

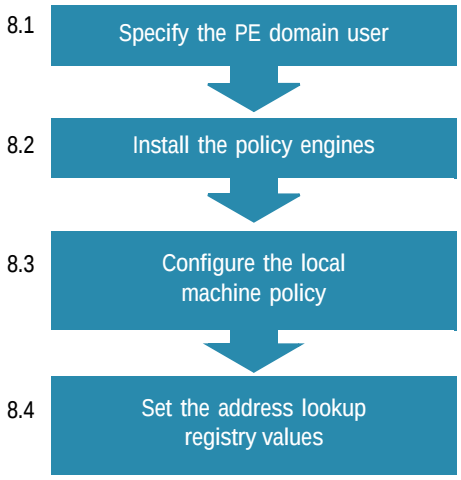
8 Policy Engines

Policy engines can process e-mail events arriving from an external 'e-mail source' and apply capture and control triggers to these e-mails where necessary.

The main purpose of policy engines is to enable Orchestria APM to integrate with Exchange Server or Lotus Domino (task 9). which in turn allows Orchestria APM to monitor and control corporate e-mail activity that would otherwise be missed by client integration alone. This includes e-mails sent using BlackBerry handhelds, Microsoft Office Outlook Web Access or Notes Web Clients. In such cases, outgoing e-mails do not pass through Microsoft Outlook or Lotus Notes and are not captured on Orchestria APM client machines.

Policy engines also underlie the Import Policy feature (task 10), which provides a mechanism for connecting Event Import to policy engines, applying policy triggers to imported e-mails directly before they are stored in the CMS.

A policy engine deployment requires the following steps. These are described on page 28.



Policy engine deployment

These steps are described on the following page.

Deployment procedure

8.1 Specify a policy engine domain user

Your policy engines must be able to access the policy engine hub. Specifically, the policy engine service must run as a domain user who can access the host machine running the policy engine hub. Likewise, the policy engine hub uses this same domain user to access the remote policy engine machines.

Therefore, you must either create a new domain user in Active Directory, or choose an existing domain user. This is your 'PE domain user'. You must also create a matching Orchestria APM user account for the policy engines to use when logging on to the CMS.

For details, see the Deployment guide; search the index for 'policy engines: user accounts'.

8.2 Install the policy engines

You install policy engines using the Orchestria APM server installation wizard. But note the requirements for the host machine. Also, the Orchestria APM Policy Engine service must log on as the PE domain user. For details, see the Deployment guide; search the index for 'policy engines: installing'.

8.3 Configure the local machine policy

After installing the policy engine and starting the service, you need to modify certain parameters in the Policy Engine folder of the local machine policy (for example, to specify how to handle unknown users). For details, see the Deployment guide; search the index for 'policy engines: machine policy settings'.

8.4 Set the address lookup registry values

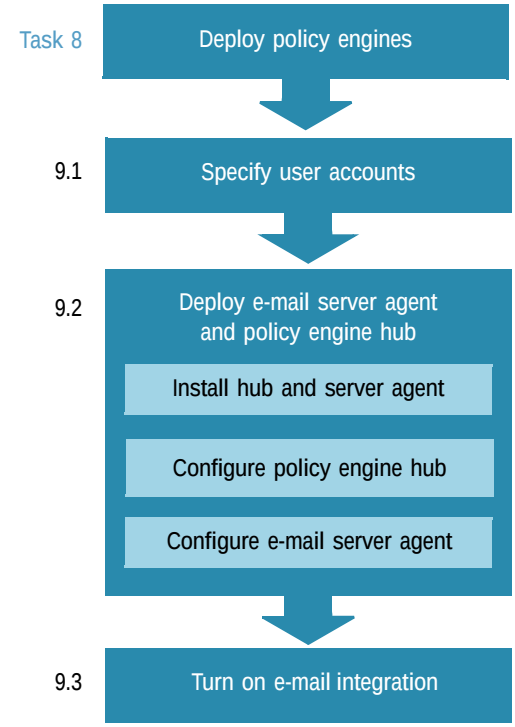
After configuring the machine policy, you may need to add registry values on the policy engine host machine. These enable the policy engine to apply the correct user policies when processing an e-mail addressed to a distribution list or an alias e-mail address. For full details, see the Deployment guide; search the index for 'policy engines: registry values'.

9 E-mail server integration

Orchestria APM can integrate with Microsoft Exchange Server and Lotus Domino. This in turn allows Orchestria APM to monitor and control corporate e-mail activity that would otherwise be missed by client integration alone. This includes e-mails sent using BlackBerry handhelds, Microsoft Office Outlook Web Access or Notes Web Clients. In such cases, outgoing e-mails do not pass through Microsoft Outlook or Lotus Notes and are not captured on Orchestria APM client machines.

After deploying your policy engines, setting up Orchestria APM integration with Exchange Server or Domino is a three-step procedure. To minimize disruption on your e-mail server, we recommend you set up the necessary user accounts first, then configure the policy engine hub, and finally the Exchange or Domino server agent. The procedure is summarized below.

For full details about each step, see the Deployment guide; search the index for 'Exchange server agent' or 'Domino server agent'.



Exchange or Domino integration: Deployment procedure.

Deployment procedure

First, you must deploy your policy engines—see task 8 on page 28. Then:

9.1 Specify the user accounts

You must first specify a domain user and a matching Orchestria APM user:

- **PE domain user:** Your policy engines and the policy engine hub use the same account to communicate with each other. This is the 'PE domain user'. This can be a new or existing domain user.
- **Orchestria APM user:** You must also create a corresponding Orchestria APM user account. Policy engines use this account to log on to the CMS when mapping e-mail addresses to Orchestria APM users.

9.2 Deploy the e-mail server agent and hub:

Briefly, you must do the following:

- **Install the hub and server agent:** These are installed together using the using the Orchestria APM Integration Agents installation wizard. After installation, you need to confirm that the hub has connected to your policy engines.
- **Configure the hub:** You must configure the policy engine hub **service** so it can log on to remote machines hosting the policy engines. You must also assign the Log on as a batch job privilege to the PE domain user on the hub host machine. Finally, you need to modify various registry values, for example, to configure size-based event queues.
- **Configure the e-mail server agent:** Again, you must modify various registry values on the server agent host machine. For example, you can tailor the server agent to only monitor e-mails sent from particular SMTP addresses or Domino domains. You can also determine how the server agent handles failures on the hub.

9.3 Turn on e-mail integration

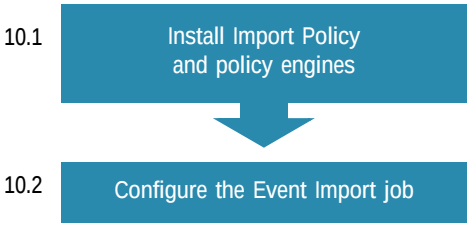
Finally, turn on Orchestria APM integration with Exchange Server or Domino. To do this, you must set the `EnableIntegration` registry value to 1. Note that changes to this value are effective immediately.

10 Import Policy

The Import Policy feature provides a mechanism for connecting Event Import to policy engines, applying policy triggers to imported e-mails directly before they are stored in the CMS. It provides organizations with a full compliance review capability that is not dependent on a preventative pre-review strategy for filtering e-mail communications at source.

Also, because Import Policy requires no integration with production e-mail systems, there is no risk of disruption to end-users' e-mail activity. Import Policy also eliminates the need for Orchestria APM client agents on the desktop and policy engines on the e-mail server. Deploying Import Policy is a two-step procedure—see below.

For full details, see the Deployment guide; search the index for 'Import Policy'.



Import Policy installation and configuration

These steps are described opposite.

Deployment procedure

10.1 Install Import Policy and policy engines

First, you must install the Policy Engine Connector and, if not already installed, one or more policy engines (see task 8 on page 28). You do this using the Orchestria APM server installation wizard.

10.2 Configure the Event Import job

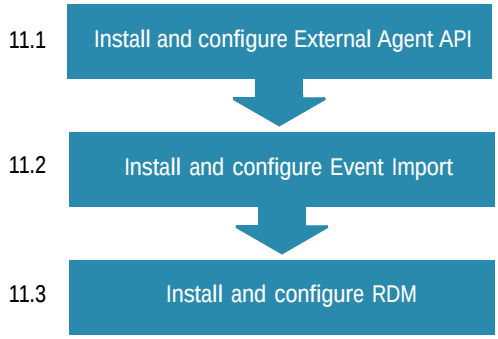
Secondly, you must configure Event Import to pass imported e-mails to a policy engine. To do this, you must configure the import parameters and start the import job. The parameters must include the usual areas (specifying the source data for the import job, e-mail address handling, and so on). The import parameters must also include the parameter:

```
Engine.UsePolicyEngineConnector=Yes
```

This parameter also supports a value of Hub, For details, see the Deployment guide; search the index for 'Event Import utility, configuration file, parameters'.

11 ZANTAZ EAS integration

Orchestria APM can integrate with the ZANTAZ EAS archive solution. An example deployment is shown on page 8. Integration is a three-step procedure:



ZANTAZ EAS integration: Deployment procedure.

For full details, see the Deployment guide; search the index for 'EAS integration'.

How the integration works

Integration with ZANTAZ EAS is provided through the External Agent API. This utility enables Orchestria APM to integrate with third party e-mail archives such as EAS.

ZANTAZ EAS connects to an e-mail server such as Microsoft Exchange and archives messages in an e-mail store. The EAS indexer process passes data to the External Agent API. The External Agent API then converts the archived e-mail into an Orchestria APM event (EVF) file along with a unique event identifier. The EVF files are saved in a cache. This cache provides the source data for Event Import, which then imports these e-mails, including the identifier, into the CMS.

Actual message data is not saved on the CMS; instead, the identifier for each imported e-mail references the associated entry in the e-mail store. The Remote Data Manager (RDM) then uses this identifier to retrieve the e-mail from the EAS archive during subsequent event searches in the iConsole or Data Management console.

Deployment procedure

11.1 Install the External Agent API

First, you need to install the External Agent API on the EAS server. You do this using the Orchestria APM Integration Agents installation wizard. When the installation is complete, you need to:

- **Configure the External Agent API**: The wizard installs the necessary DLLs and registry values to the External Agent API host machine. For example, it adds registry values to specify the path to the EVF file cache and the minimum level of free disk space on the cache host machine. If required, you can modify the default registry settings.

- **Edit the EAS.INI file**: Next, you must now edit the EAS.INI file, specifying the full path to External Agent API, wgnrdi.dll.

- **Start up the External Agent API**: After installing the External Agent API, you need to run the EAS indexer process. This causes the External Agent API to start converting messages from the e-mail archive and saving them in the EVF file cache.

11.2 Install Event Import

The Event Import utility retrieves the extracted e-mails from the EVF fie cache specified in step **11.1** and imports them into the CMS. For details about installing Event Import machines, see task 7 on page 26.

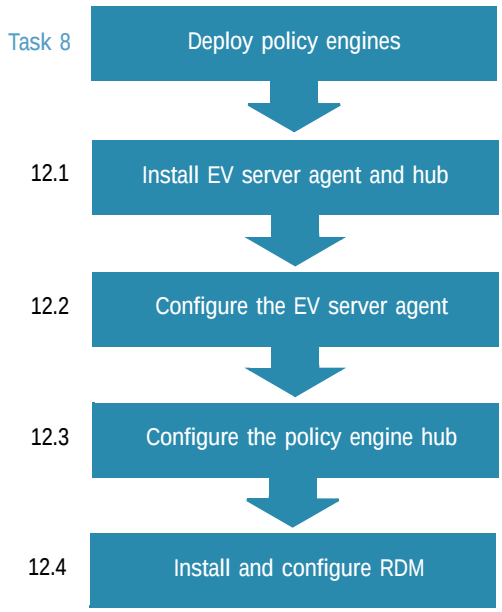
11.3 Install and configure RDM

Finally, you need to install the RDM. This utility enables Orchestria APM to retrieve events archived in third party remote storage locations and display them in the Data Management console or iConsole.

When installing the RDM, you need to select ZANTAZ EAS from the archive list when you run the Orchestria APM server installation wizard—see step 18 on page 39.

12 Enterprise Vault integration

Orchestria APM can integrate with the Symantec Enterprise Vault archive solution. It intercepts e-mails extracted from a journal mailbox in Microsoft Exchange and applies smart tags to these e-mails before they are archived in Enterprise Vault. Integration involves the following steps:



Enterprise Vault integration: Deployment procedure

For full details, see the Deployment guide; search the index for 'Enterprise Vault integration'.

How the integration works

Integration is provided through an Orchestria APM custom filter (the 'EV server agent'). When integration is enabled, Enterprise Vault notifies the EV server agent when it extracts an e-mail from a Microsoft Exchange journal mailbox. The EV server agent passes a copy of the e-mail to the policy engine hub.

The hub allocates the e-mail to a policy engine, which then applies the appropriate smart tags to the e-mail (typically an e-mail category and a retention date) and passes this data in a callback to the EV server agent and then to Enterprise Vault. Finally, Enterprise Vault archives the e-mail along with its smart tag details.

Processed events, including an identifier, are then replicated from the policy engine up to the CMS. Actual message data is not saved on the CMS; instead, the identifier for each e-mail references the associated entry in the Enterprise Vault archive. The Remote Data Manager (RDM) then uses this identifier to retrieve the e-mail from the archive during subsequent event searches in the iConsole or Data Management console.

About Smart Tagging

Smart Tagging is an innovative feature that enables Orchestria APM to accurately categorize events at the time of capture. A setting in each policy trigger defines a smart tag. For example, you can assign smart tags such as 'Privileged Content' or 'Employment Solicitation'. When the trigger activates, this tag is saved with the event metadata in the CMS database. It is also passed back to Enterprise Vault to be archived with the e-mail.

Deployment procedure

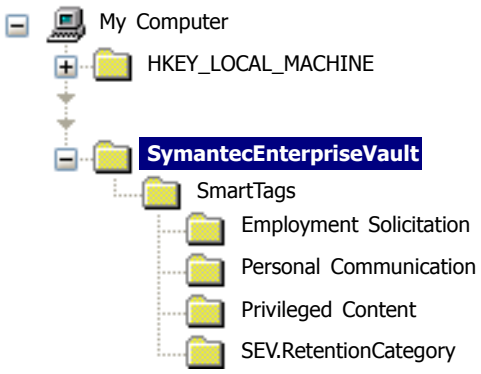
First, you must deploy your policy engines—see task 8 on page 28. Then:

12.1 Deploy the EV server agent and policy engine hub

You install the EV server agent using the Orchestria APM Integration Agents installation wizard. In the Custom Setup screen, choose the Symantec Enterprise Vault feature. The policy engine hub is installed automatically with this feature.

12.2 Configure the EV server agent

You configure the EV server agent by editing the registry on the host server. In particular, you need to specify how EV server agent handles event failures, out-of-memory failures, and smart tags with multiple values. The key structure is shown below:



Enterprise Vault integration: registry key structure

12.3 Configure the policy engine hub

You must configure the policy engine hub **service** so it can log on to remote machines hosting the policy engines. You must also assign the Log on as a batch job privilege to the PE domain user on the hub host machine.

Finally, you need to modify various registry values, for example, to configure how policy is applied to e-mails from unrecognized senders, and to specify logging details or size-based event queues.

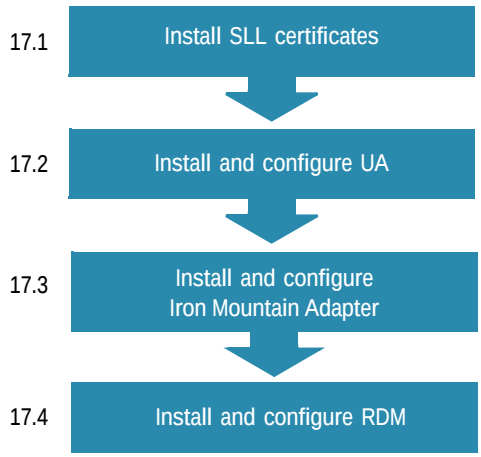
12.4 Install and configure RDM

Finally, you need to install the RDM. This utility enables Orchestria APM to retrieve events that are archived in third party remote storage locations and display them in the Data Management console or iConsole.

When installing the RDM, you need to select Symantec Enterprise Vault from the archive list when you run the Orchestria APM server installation wizard—see step 18 on page 39.

13 ZANTAZ Digital Safe integration

Orchestria APM can integrate with ZANTAZ Digital Safe archives. E-mails extracted from a journal mailbox in Microsoft Exchange are intercepted and forwarded to a Digital Safe archive:



ZANTAZ Digital Safe integration: Deployment procedure.

For full details, see the Deployment guide; search the index for 'Digital Safe integration'.

How the integration works

The UA extracts e-mails from Exchange mailboxes and outputs them to a Digital Safe Adapter. This outputs the e-mails to the Digital Safe archive. The archive then sends event and archive identifiers back to the UA.

After confirmation that an e-mail has been successfully archived, the UA outputs a copy of the e-mail to an EVF file for subsequent importing into the CMS. The EVF file includes the event and archive identifiers that reference the associated entry in the Digital Safe archive.

A second Digital Safe Adapter typically runs on the CMS. During event searches, the RDM passes the event identifiers to this second Digital Safe Adapter, which in turn retrieves e-mails stored in the Digital Safe archive and pass them back to the RDM.

Deployment procedure

13.1 Install SSL certificates: These certificates are used to enable secure communication between Orchestria APM and Digital Safe. You need to acquire, import and register SSL authentication certificates for the Digital Safe Adapter. This complex procedure is described in the *Deployment guide.*

13.1 Install and configure the Universal Adapter
This requires the following steps:

- **Specify the UA domain user:** The UA service must run as a domain user who can access the relevant mailboxes hosted on the Exchange server.
- **Install a de-duplication database:** This step is optional. A de-duplication database enables the UA to detect and remove duplicate e-mails.
- **Install the Universal Adapter:** Run the Orchestria UA installation wizard.
- **Configure the Universal Adapter:** You need to edit the registry on the UA host machine. Output registry values define an interface to an Iron Mountain digital archive; input registry values specify which journal mailboxes the UA is importing from.

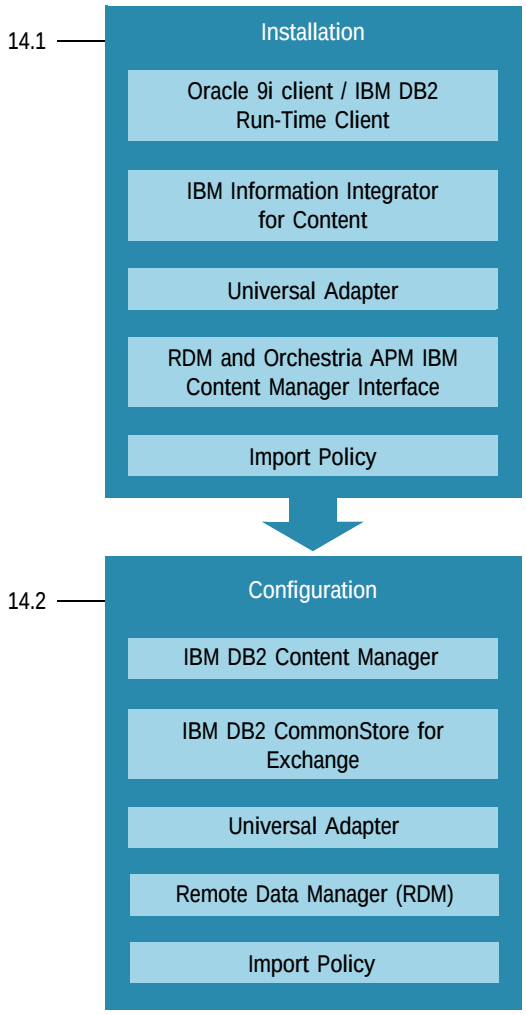
13.2 Install and configure the Iron Mountain Adapter
This requires the following steps:

- **Install the Iron Mountain Adapter:** Use the Orchestria APM Integration Agents installation wizard. In the Custom Setup screen, choose the Iron Mountain Integration feature..
- **Configure the Iron Mountain Adapter:** Registry values on the host server enable secure communication with the Iron Mountain digital archive. For example, you must identify the SSL certificate used to authenticate wgnirm.dll to the archive.

13.3 Install and configure RDM
The RDM enables Orchestria APM to retrieve events that are archived in third party remote storage locations and display them in the Data Management console or iConsole during event searches. For details, see step 18 on page 39.

14 IBM DB2 CommonStore for Exchange integration

Orchestria APM integration with IBM DB2 CommonStore for Exchange is provided through the Universal Adapter (UA) and involves the following tasks:



IBM DB2 CommonStore for Exchange integration procedure

How the integration works

With this type of integration, the UA ingests e-mails from one or more Exchange Journals and outputs them, each with a unique ID, to one or more Exchange mailboxes. IBM DB2 CommonStore for Exchange can then archive the e-mails. The UA also outputs the same e-mails to an event cache for subsequent import into the CMS, via Import Policy. The import operation ensures that policy is applied to events corresponding to e-mails in the archive. The archived e-mails can be subsequently retrieved by reviewers using Orchestria APM consoles, retrieving the actual e-mail content message data from the IBM DB2 Content Manager.

Deployment procedure

14.1 Install the following:

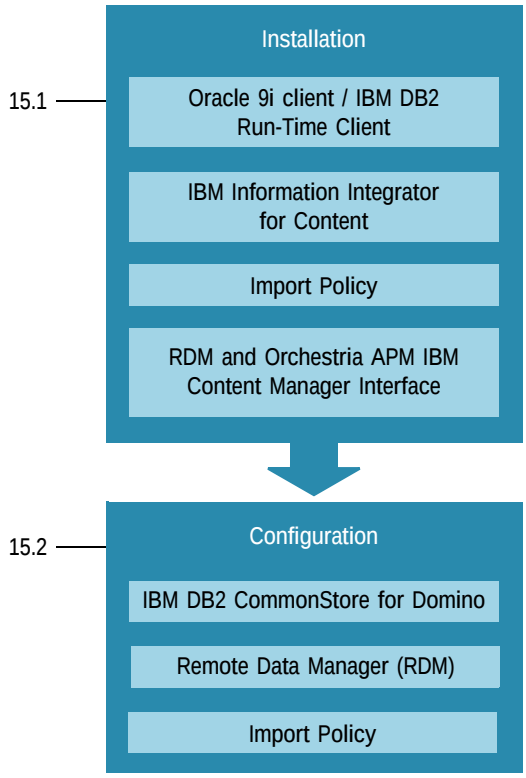
- **Oracle 9i client or IBM DB2 Run-Time Client:** Install the database client that corresponds with your installation of IBM DB2 Content Manager.
- **IBM Information Integrator for Content:** This must be installed on the RDM server *before* installing RDM.
- **Universal Adapter:** This must be installed on a separate machine and configured to retrieve e-mails from the Exchange Journal, and forward them on an Exchange mailbox.
- **RDM and Orchestria APM IBM Content Manager Interface:** Install these using the Orchestria APM server installation wizard.
  When installing the RDM, you need to select IBM CommonStore from the archive list when you run the Orchestria APM server installation wizard—see step 18 on page 39.
- **Import Policy:** Install using the Orchestria APM server installation wizard. For details, see page 30.

14.2 Configure the following:

- **IBM DB2 Content Manager** to recognize the unique ID added to each e-mail by the UA.
- **IBM DB2 CommonStore for Exchange** to treat the unique ID generated by the UA as an indexed property.
- **UA** to intercept e-mails from an Exchange Journal and pass them on to an Exchange Mailbox.
- **RDM** to retrieve e-mails from the IBM DB2 Content Manager during an event search.
- **Import Policy** to take EVF files and create Orchestria APM events from them.

15 IBM DB2 CommonStore for Lotus Domino integration

Integrating Orchestria APM with IBM DB2 CommonStore for Domino involves the following tasks:



IBM DB2 CommonStore for Domino integration procedure

How the integration works

IBM DB2 CommonStore for Domino ingests e-mails from a Notes Journal Database on a Lotus Domino Server. There they are each given a unique 'Archive ID' which is stored as a property of the e-mail. Import Policy then imports all e-mails with an Archive ID, applies policy and replicates them up to the CMS.

The import operation ensures that policy is applied to events corresponding to e-mails in the archive. The archived e-mails can be subsequently retrieved by reviewers using Orchestria APM consoles, retrieving e-mail content from the IBM DB2 Content Manager if the CMS remote data cache does not contain a copy.

Deployment procedure

15.1 Install the following:

- **Oracle 9i client or IBM DB2 Run-Time Client:** Install the database chosen for use with IBM DB2 Content Manager.
- **IBM Information Integrator for Content:** This IBM component must be installed on the RDM server *before* you install RDM.
- **Import Policy:** This utility retrieves e-mails from the Notes Mail Journal, applies policy to them and then imports them into the CMS.

  You also need to install a Notes Client on the Import Policy machine.
- **RDM and Orchestria APM IBM Content Manager Interface:** Install these using the Orchestria APM server installation wizard.

  When installing RDM, you need to select IBM CommonStore from the archive list when you run the Orchestria APM server installation wizard—see step 18 on page 39.

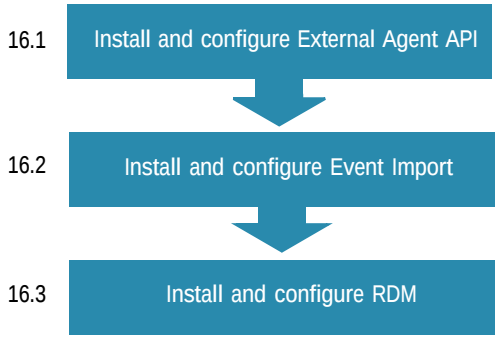
  You also need to install a Notes Client on the RDM machine.

15.2 Configure the following::

- **IBM DB2 CommonStore for Domino** to integrate with Orchestria APM. For details, see the Deployment guide.
- **RDM** to communicate with IBM DB2 CommonStore for Domino and retrieve e-mails from the IBM DB2 Content Manager during an event search.
- **Import Policy** to import e-mails from the Notes database(s) that you have configured in the CSLDConf Automated Archiving Database Set.

16 EMC EmailXtender integration

Orchestria APM can integrate with the EMC EmailXtender archive solution. An example deployment is shown on page 8. Integration is a three-step procedure:



EMC EmailXtender integration: deployment procedure.

For full details, see the Deployment guide; search the index for 'EMC EmailXtender integration'.

How the integration works

Integration with EMC EmailXtender is provided through the External Agent API. This utility enables Orchestria APM to integrate with third party e-mail archives such as EMC.

EMC EmailXtender connects to an e-mail server such as Microsoft Exchange and archives messages in an e-mail store. The EMC archive then passes data to the Orchestria APM External Agent API. The External Agent API then converts the archived e-mail into an Orchestria APM event (EVF) file along with a unique event identifier. The EVF files are saved in a cache. This cache provides the source data for Event Import, which then imports these e-mails, including the identifier, into the CMS.

Actual message data is not saved on the CMS; instead, the identifier for each imported e-mail references the associated entry in the e-mail store. The Remote Data Manager (RDM) then uses this identifier to retrieve the e-mail from the EMC archive during subsequent event searches in the iConsole or Data Management console.

Deployment procedure

16.1 Install the External Agent API

First, you need to install the External Agent API on the EMC EmailXtender server. You do this using the Orchestria APM Integration Agents installation wizard. When the installation is complete, you need to:

- **Configure the External Agent API**: The wizard installs the necessary DLLs and registry values to the External Agent API host machine. For example, it adds registry values to specify the path to the EVF file cache and the minimum level of free disk space on the cache host machine. If required, you can modify the default registry settings.

- **Further External Agent API configuration:** If you are integrating with EMC EmailXtender, please contact the Orchestria service desk—see page 5.

- **Start up the External Agent API**: After installing the External Agent API, you need to run the EMC EmailXtender process. This causes the External Agent API to start converting messages from the e-mail archive and saving them in the EVF file cache.

16.2 Install Event Import

The Event Import utility retrieves the extracted e-mails from the EVF fie cache specified in step **16.1** and imports them into the CMS. For details about installing Event Import machines, see task 7 on page 26.

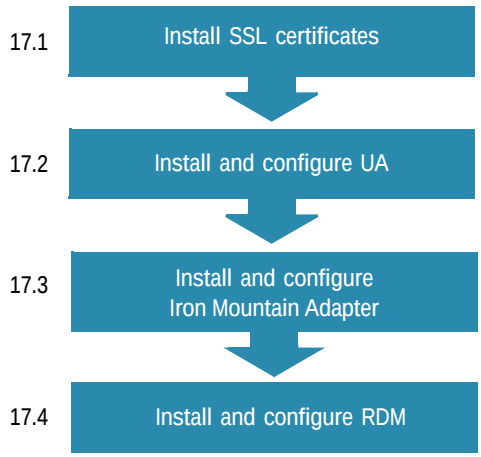
16.3 Install and configure RDM

Finally, you need to install the RDM. This utility enables Orchestria APM to retrieve events archived in third party remote storage locations and display them in the Data Management console or iConsole.

When installing the RDM, you need to select EMC EmailXtender from the archive list when you run the Orchestria APM server installation wizard—see step 18 on page 39.

17 Iron Mountain integration

Orchestria APM can integrate with Iron Mountain digital archives. E-mails extracted from a journal mailbox in Microsoft Exchange are intercepted and forwarded to an Iron Mountain digital archive:



Iron Mountain integration: Deployment procedure.

For full details, see the Deployment guide; search the index for 'Iron Mountain integration'.

How the integration works

The UA extracts e-mails from Exchange mailboxes and outputs them to an Iron Mountain Adapter. This uses the Iron Mountain Ingestion service to output the e-mails to the Iron Mountain digital archive. The archive then sends event and archive identifiers back to the UA.

After confirmation that an e-mail has been successfully archived, the UA outputs a copy of the e-mail to an EVF file for subsequent importing into the CMS. The EVF file includes the event and archive identifiers that reference the associated entry in the Iron Mountain archive.

A second Iron Mountain Adapter typically runs on the CMS. During event searches, the RDM passes the event identifiers to this second Iron Mountain Adapter, which in turn uses the Iron Mountain Retrieval service to retrieve e-mails stored in the Iron Mountain digital archive and pass them back to the RDM.

Deployment procedure

17.1 Install SSL certificates: These certificates are used to enable secure communication between Orchestria APM and Iron Mountain. You need to acquire, import and register SSL authentication certificates for the Iron Mountain Adapter. This complex procedure is described in the *Deployment guide.*

17.2 Install and configure the Universal Adapter

This requires the following steps:

- **Specify the UA domain user:** The UA service must run as a domain user who can access the relevant mailboxes hosted on the Exchange server.
- **Install a de-duplication database:** This step is optional. A de-duplication database enables the UA to detect and remove duplicate e-mails.
- **Install the Universal Adapter:** Run the Orchestria UA installation wizard.
- **Configure the Universal Adapter:** You need to edit the registry on the UA host machine. Output registry values define an interface to an Iron Mountain digital archive; input registry values specify which journal mailboxes the UA is importing from.

17.3 Install and configure the Iron Mountain Adapter

This requires the following steps:

- **Install the Iron Mountain Adapter:** Use the Orchestria APM Integration Agents installation wizard. In the Custom Setup screen, choose the Iron Mountain Integration feature.
- **Configure the Iron Mountain Adapter:** Registry values on the host server enable secure communication with the Iron Mountain digital archive. For example, you must identify the SSL certificate used to authenticate wgnirm.dll to the archive.

17.4 Install and configure RDM

The RDM enables Orchestria APM to retrieve events that are archived in third party remote storage locations and display them in the Data Management console or iConsole during event searches. For details, see step 18 on page 39.

18 Remote Data Manager

The Remote Data Manager (RDM), Wgnrdm.dll, enables Orchestria APM to retrieve events that are archived in third-party remote storage locations and display them in the iConsole or Data Management console. An example RDM deployment is shown on page 8.

Deployment procedure

18.1 Install the RDM:

The RDM host machine must have a Microsoft Exchange-compatible application installed, such as Outlook 2003.

To install the RDM, you use the Orchestria APM Integration Agents installation wizard. In particular:

- In the Custom Setup screen, choose the Remote Data Manager feature.
- the Service Accounts screen, specify the logon account used by the Orchestria APM infrastructure service. This account requires the 'Log on as a service' security privilege—see step 18.2.
- In the Remote Data Manager Configuration screen, specify the target archive. The current release supports ZANTAZ EAS and Digital Safe, Enterprise Vault, EMC EmailXtender, IBM DB2 and Iron Mountain.

Note there are additional requirements for EAS integration. For full instructions, see the Deployment guide; search the index for 'RDM'.

18.2 Assign the 'Log on as a service' privilege to the infrastructure logon account:

1 Ensure that you are logged on with local administrator rights on the RDM host machine.

2 Open the Local Security Policy applet or, if this machine is a domain controller, open the Domain Controller Security Policy applet. Both applets are available in Administrative Tools.

3 Expand the Local Policies branch and select User Rights Assignment. This security area determines which users have logon privileges on the local computer.

4 Assign the 'Log on as a service' privilege to the Orchestria APM infrastructure logon account.

18.3 Confirm that the installation succeeded

In the Windows Services applet, confirm that these services have started. To do this:

1 Open an Administration console and expand the My Servers list .

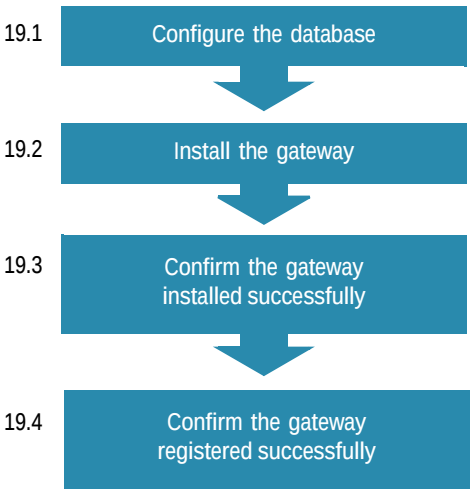
2 Select the parent CMS .

3 The Server Machine screen lists all utility services parented to this CMS. The RDM will be listed here.

19 Gateway installation

Gateways are optional data-routing servers, operating between the CMS and client machines. The parent is either the CMS or another gateway. This type of hierarchical, distributed deployment provides resilience and network load-balancing.

Typically, you only deploy gateways if you are also deploying Orchestria APM client machines. First, you must install and configure a database on the target server. Then you can install the gateway itself. Finally, you need to confirm that the installation was successful.



Gateway installation and configuration

These steps are described below.

Installation procedure

19.1 Configure the database

Create a new database for Orchestria APM. Then, as for the CMS, create a user or login that Orchestria APM can use to access the gateway database. For database configuration and optimization guidelines, see the references in task 1 on page 16.

19.2 Install the gateway

Use the Orchestria APM server installation wizard. For installation instructions, see the Deployment guide; search the index for 'gateway servers: Linux, Solaris or Windows: installing'.

19.3 Confirm that the gateway installed successfully

In the Windows Services applet, confirm that the Orchestria APM infrastructure service has started.

If the installation failed, check the Orchestria APM 'Activity' and 'System' logfiles for any error messages. For details, see step **2.2** on page 18.

19.4 Confirm the gateway registered successfully

You need to confirm that the gateway has correctly registered with the CMS. To do this, open an Administration console:

i) Expand the My Servers list and connect to the parent CMS.

ii) Expand the Machine Administration branch. The new gateway will be listed under the CMS.

The new gateway will automatically inherit the common gateway policy, as defined in CMS step **2.4** *on page 18.*

Unattended installations

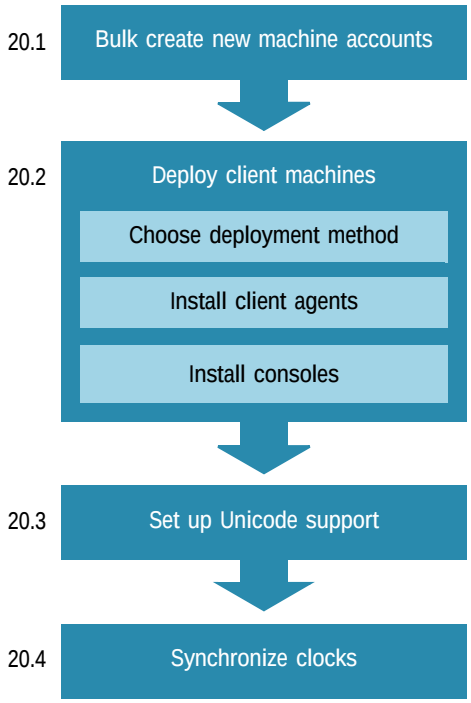
You can also configure an unattended installation using command line options for msiexec.exe, the Microsoft Windows Installer service. Orchestria APM supports a range of variables that you can use as msiexec.exe parameters. For details, see the Deployment guide; search the index for 'unattended installations'.

Support for Unicode characters

All Orchestria APM consoles now support Unicode character sets. To implement Unicode support on Oracle gateways, you need to set up the database for Orchestria APM to use UTF-8 encoding for the DBMS code page. For full details, see the Deployment guide; search the index for 'Unicode characters: general configuration'.

20 Client deployment

Client machines are computers used by Orchestria APM users. They host Orchestria APM client agents and, optionally, consoles. These client agents enable Orchestria APM to integrate with e-mail and browser applications on the client machine, and to detect when other specified applications are being used. Orchestria APM supports a range of client installation methods. You can also bulk create accounts for new client machines before rolling out the client software. The overall procedure is summarized below:



Client machines: Deployment procedure
These steps are described opposite.

Installation procedure

20.1 Bulk create new machine accounts

To simplify mass deployments, you can optionally bulk create new machine accounts and pre-assign client machines to parent servers in advance of the Orchestria APM rollout. This enables you to deploy multiple client machines using a single source image (which identifies a single parent server) whilst ensuring that each client machine automatically connects to its 'correct' parent server immediately after installation. See the Deployment guide; search the index for ‘Account Import: machines’.

20.2 Deploy the client machines

When you roll out Orchestria APM to your client machines, you need to:

i) Choose a deployment method.

ii) Decide which client agents to install.

iii) Identify which machines will host Orchestria APM consoles.

These issues are discussed below. For full details, see the Deployment guide; search the index for ‘client machines: installation’.

i) Deployment method

Orchestria APM supports various manual and command line deployment operations, plus managed methods of installing to multiple clients:

- **Managed operations:** These enable you to simultaneously install multiple client machines. The main supported methods are Windows 2000 Group Policy, Microsoft SMS and ‘snapshot’ deployments (also called ‘ghost imaging’).
- **Command line operations:** Orchestria APM installs using the Microsoft Windows Installer service. This enables you to use the command line options of msiexec.exe to install or uninstall.
- **Manual operations:** You can manually install or uninstall Orchestria APM from individual client machines using the installation wizard, setup.exe.

ii) Install client agents

Orchestria APM client agents can integrate with e-mail and browser applications on the client machine, and to detect when other specified applications are being used. Client agents include:

- **Microsoft Internet Explorer Integration:** This enables capture or control of any Web activity in Internet Explorer or Windows Explorer.
- **Microsoft Outlook Integration:** This enables capture or control of any Outlook-based e-mail activity. If both the Outlook and Internet Explorer integration features are installed, Orchestria APM can also capture or control any Web activity when Outlook is used as a Web browser.
- **Lotus Notes Integration:** This enables capture or control of any Notes-based e-mail activity.
- **Application Integration:** This enables Orchestria APM to monitor usage of other desktop applications and capture application usage metrics.

iii) Install consoles

You administer Orchestria APM using consoles. You can install console on any Orchestria APM machine. The following consoles are available:

- **Administration console:** This enables you to administer user and machine accounts, manage policies and configure statistics.
- **Data Management console:** This allows users to search for, review and audit captured data.
- **Executive console:** This provides real time tracking of Web and e-mail activity. It is designed for executives and other senior decision-makers.

20.3 Set up support for Unicode characters

All Orchestria APM consoles now support Unicode character sets. For example, it is now possible in the Data Management console to search for e-mails containing strings of Far Eastern characters. You need to implement Unicode support on all Orchestria APM client machines that are likely to capture e-mails and other events that contain Far Eastern text. You must also implement Unicode support on all client machines running an Orchestria APM console and which are likely to display events or user names that contain Far Eastern characters.

For full details, see the Deployment guide; search the index for ‘Unicode characters: general configuration’.

20.4 Synchronize the machine clocks

When an event is are captured on a client machine, it is time stamped. This time stamp is preserved when the event is replicated up to the CMS. For this reason, it is important that all of your Orchestria APM machines are set to the correct date and local time. This normally happens automatically. Machine clocks are typically synchronized automatically by a network time server or, for machines not in a domain, by an Internet time server. But if an Orchestria APM machine does not have a continuous Internet connection, this automatic synchronization may not occur. Make sure the owners of these machines understand the need to keep their machine set to the correct date and time.

For full details, see the Deployment guide; search the index for ‘clock synchronization’.

Index