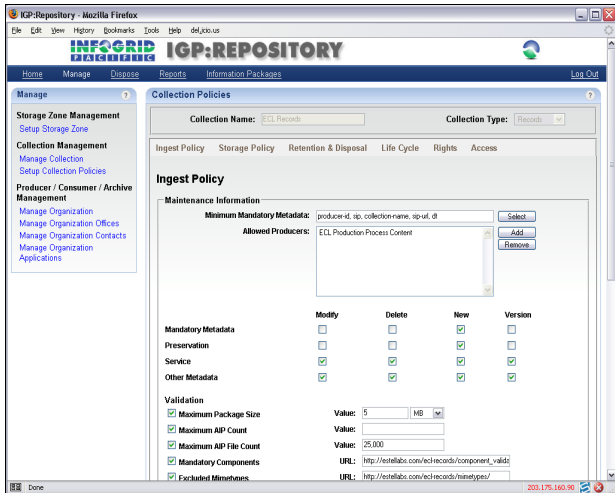
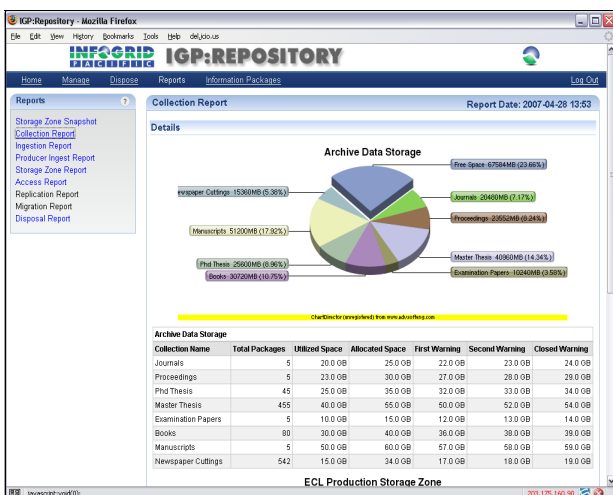


A trustworthy digital archive for documents, records, archives, images, A/V and any other digital data



Complex archive policies are simply created from one unified interface and enforced automatically across the system

- ▶ Self replicating multi-site storage
- ▶ Compliant Records Management
- ▶ Retention & Disposal policies
- ▶ Document and all data archiving
- ▶ OAIS Digital Preservation Archive
- ▶ Data cache storage mode
- ▶ Powerful admin and reporting
- ▶ Replication, migration built-in
- ▶ Comprehensive audit logs



Powerful reporting and Archive Administration features allow you to understand what is happening in your storage system at any time

Overview

IGP:Repository 2 is a stable, trusted and effective storage system for easily deployed, extensible and affordable digital content archiving strategies including:

- Records management for any organization (ISO 15489 and DoD 5051)
- Digital Preservation archive for libraries, museums, archives, and enterprise of all types (TRAC certification ready)
- General documents, and other files such as audio, video and datasets
- High turnover cache data management such as temporary backups or fast changing production data sets

IGP:Repository 2 is a practical implementation of the OAIS (Reference Model for an Open Archival Information System). It integrates seamlessly with IGP:InfoViewer 2 for controlled Online access to the stored content, and IGP:Production Solutions where high volume content digitization and creation is needed.

IGP:Repository brings the concepts of CDP (Continuous Data Protection) to organizations of all types. The live replication features ensure 100% uptime and 100% data availability.

Types of Archiving Supported

IGP:Repository can be configured to support a wide range of archiving activities including:

Controlled Access Repository A controlled access repository has as its focus stringent requirements for auditability, authentication, and access controls. This is useful in records management and other statutory compliance requirements.

Data Model Archive To preserve specific types of data for future reuse. The architecture scales to almost any size and it supports automated acquisition, quality control, and description.

Archive of Temporally Changing Data Preserve data that is continually changing, either through regular additions that are streamed into the archive or through updates and changes.

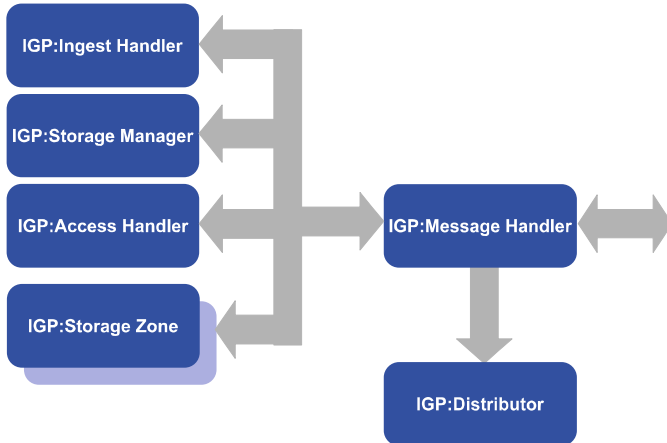
Archive of Derived Data Products Preserve and manage original data, while storing related processing data sets or derived content objects.

Ingest and Access Options

- IGP:Metadesk for desk to archive ingest
- IGP:Process Content for high volume ingest
- IGP:InfoViewer 2 forms and catalogs
- Other applications using REST and SOAP protocols

Modules

IGP:Repository 2 consists of four major modules which can be deployed on one or multiple servers. They communicate using *IGP:Message Handler* which authenticates and authorizes all participating applications through *IGP:Distributor*. All modules are full Web Services and can be load balanced and clustered together or individually for unlimited expansion and performance enhancement.



IGP:Storage Manager

The Storage Manager module implements the archive administration and management policies and tracks all repository activity. It contains a full map of all data across any number of sites, and asserts storage and retrieval policies at the file and data level.

IGP:Storage Zone

The files are stored in any number of independent Storage Zones. Storage Zones can be in separate geographical locations allowing the implementation of a multi-site disaster recovery strategy.

IGP:Ingest Handler

The Ingest Handler provides the producer submission address and input point for the archive. Carries out Submission Information Package (SIP) conformance checking to ensure compliance with the archive ingestion policies. IGP:Ingest Handler also enforces copy, version and revision control strategies against authorized system users.

IGP:Access Handler

IGP:Access Handler enforces the archive access policies to enforce User-Archive access and distribution policies through OAIS DIPs (Dissemination Information Packages) created from AIPs and METS Structure maps.

IGP:Search

Documents of all types can be automatically indexed by metadata and full text as they are ingested. Search is accessible as a Web Service supporting multiple languages.

Search options include: Simple, phrase search and query search, Boolean AND, "+" OR, NOT, and "-" plus mixed expressions, Wildcard, proximity and fuzzy searches, Search Term Boosting, term grouping, Unicode compliance and multiple languages

IGP:Archive Administrator

The Browser Administration Interface allows single point control of all Ingest, Storage and Access policies.

It provides a single point for archive life-cycle maintenance activities such as replication, migration, data validation,

retention and disposal actions, reporting and other services. The administrator has complete control over producer (who can put content into the system) and consumer (who can take content out of the system) policies by collection.

Information Packages for Survivability

IGP:Repository 2 uses an OAIS structured Archive Information Package (AIP) to store information in the system with using custom METS (Metadata for Encoding and Transmission Standard) profiles. This contains the full metadata of each data item being stored, as well as the reference to the individual data objects. Standard METS profiles are included.

Automation through Policies

IGP:Repository 2 is a policy driven framework. That means you set up the business rules for each collection, and the application will enforce them consistently without human intervention. Policies include:

Ingest Policies include: Producer authorization, file actions, validation based on multiple criteria, SIP to AIP repackaging, file processing, search and indexing rules.

Storage Policies include: Setup of Storage Zones and Collection, number of replications, storage warning limits

Retention & Disposal Policies include: Retention triggers, types and periods, disposal actions, options, review notifications.

Life-cycle Policies include: surface refresh, replication and migration

Rights Policies include: can the content be distributed?

Access Policies include: Consumer authorization, DIP generation rules, access type (http, ftp, rsync), auto policy for *IGP:InfoViewer 2*

Software and Hardware Requirements

Operating System & Software

- Operating Systems Linux (Kernel 2.6) (can be deployed on Windows)
- Default database PostgreSQL 8.2
- Web Framework Django 1.0
- Web Server Apache
- 150MB common application software library space on hard disk
- 5MB application space on hard disk
- Single site license for any number of servers and users

Recommended Server Hardware

- 32/64 bit Processor
- 1GB RAM minimum. 2GByte RAM strongly recommended for single server deployments
- Special high-volume storage device configurations will be required
- (Large scale IGP:Repository 2 deployments use multiple servers)



Infogrid Pacific Pte Ltd

Singapore/ SE Asia:	Joseph Yeo	+65 94595939
NZ, Oceania:	Andrew Crisp	+64 (0) 216 54397
India/South Asia:	Richard Pipe	+91 (20) 329 12384
London, UK:	Karlie Ritchie	+44 (0) 798 370 8460

Email: sales@infogridpacific.com
Internet: <http://www.infogridpacific.com>