CONCEPTS GUIDE

Axway 5 Suite

Managed File Transfer

6 February 2016

This documentation describes the following Axway software:

Axway 5 Suite

Contents

Preface

This guide describes the Managed File Transfer reference solution.

Who should read this guide

This guide is intended for enterprise architects, enterprise personnel involved in the implementation project, and Axway Professional Services personnel.

Familiarity with Axway 5 Suite products is recommended.

How to use this guide

The following is a brief description of the contents of each chapter:

MFT concepts – Introduces the reference solution and its use cases. For more information, see *MFT concepts* on page 8.

MFT use cases – Describes the relevant use cases for this reference solution. For more information, see *MFT use cases* on page 9.

MFT features and services – Contains information on the features and services provided by the reference solution. For more information, see *MFT features and services* on page 11.

MFT products – Describes the products provided by the reference solution. For more information, see *MFT products* on page 14.

How the products work together – Describes how the products work together in the context of data flows, access management, and visibility. It also contains basic architectural examples of the reference solution. For more information, see *How the products work together* on page 18.

Glossary – Contains a list of terms used in this guide and their definitions.

Axway 5 Suite documentation

The Axway 5 Suite documentation set includes the following guides:

- *Axway 5 Suite Supported Platforms*

  Lists the different operating systems, databases, browsers, and thick client platforms supported by each product in Axway 5 Suite.

- *Axway 5 Suite Interoperability Matrix*

  Provides product version and interoperability information for products used in an Axway 5 Suite reference solution.

- *Axway 5 Suite Upgrade Guide*

  Provides upgrade information for a subset of Axway 5 Suite products.

Axway 5 Suite reference solution guides provide conceptual information about the reference solution, and information about use cases, how the products work together, and so much more:

- *B2B Integration Concepts Guide*
- *Managed File Transfer Concepts Guide*
- *Accounting Integration Concepts Guide*
- *Financial Integration Implementation Guide*

Note A complete documentation set for each product is available on Axway Sphere at https://support.axway.com.

Training services

Axway offers training across the globe, including on-site instructor-led classes and self-paced online learning. For details, go to: http://www.axway.com/support-services/training.

Support services

The Axway Global Support team provides worldwide 24 x 7 support for customers with active support agreements.

Email support@axway.com or visit Axway Sphere at https://support.axway.com.

Accessibility

Axway strives to create accessible products and documentation for users.

This documentation provides the following accessibility features:

- Screen reader support
- Support for high contrast and accessible use of colors

Screen reader support

- Alternative text is provided for images whenever necessary.
- The PDF documents are tagged to provide a logical reading order.

Support for high contrast and accessible use of colors

- The documentation can be used in high-contrast mode.
- There is sufficient contrast between the text and the background color.
- The graphics have the right level of contrast and take into account the way color-blind people perceive colors.

MFT concepts 1

Managed File Transfer is the combination of products used to transmit data from one or more sources to one or more destinations when the data payload is unchanged. Managed File Transfer provides services that enable you to manage, secure, and monitor the exchange of large volumes of data between entities, such as organizations, persons, or applications. The use cases Managed File Transfer addresses are:

- Application-to-application (A2A) transfers – Characterized by data exchanges between applications within an enterprise that use certain sets of protocols.
- Business-to-business (B2B) Internet-based transfers – Characterized by data exchanges with external businesses – or business participants – that use various standards.
- Human-to-human and human-to-system (Human2*) transfers – Characterized by data exchanges either initiated or acted upon by a person in an ad hoc manner.

MFT use cases 2

This section describes the following MFT use cases:

- Managed file transfer consolidation or shared service
- Modernization and differentiation

Managed file transfer consolidation or shared service

This use case applies to A2A, B2B, and Human2* transfers and is also referred to as "FTP replacement".

Organizations recognize that "file-based integration" is a critical integration pattern to support their business, and they also recognize the need to secure data, control costs, and manage the partner life cycle. They may also want to provide MFT services to multiple lines of business, often charging back or selling the service internally to show benefits of visibility, reliability, and governance from a central point within the organization. Through this type of consolidation and shared service offering, the organization can:

- Lower costs by reducing the number of data centers and MFT tools
- Improve security and support new file transfer needs including cloud and mobile
- Reduce the cost of creating and managing connections
- Ease the complexity of file transfer exchanges with non-compliant platforms
- Track end-to-end all transactions across highly distributed networks with multiple routing workflows
- Support better file management and ad hoc messaging

Managed File Transfer addresses these needs by providing:

- The ability to centrally govern, manage data flows and monitor compliance. This leads to improved security through standardization and centralized control.
- An integrated file management platform to provide centralized governance of file movements.
- Ad hoc, asynchronous, human-to-system, and automated file transfer.

Modernization and differentiation

Applies to both A2A and B2B transfers and is also referred to as "store-to-corporate".

Large retail organizations that have broad distribution networks move significant amounts of data between corporate headquarters and retail outlets to support inventory, in-store services, store closing data, card processing, and so on. These types of data transfer all require interactions between corporate functions, such as resource planning, and the retail outlets.

The nature of this data is critical to providing the best in-store experience for customers, as well as for complying with payment card industry (PCI) standards and other requirements. In addition, the need for cost controls and efficiency in retail operations demand governance of data flow and audit of interactions.

Managed File Transfer addresses these needs by providing:

- The ability to centrally govern, manage data flows and monitor compliance. This leads to improved security through standardization and centralized control.
- An integrated file management platform to provide reliability and visibility on sales and stock levels for semi-automatic stock replenishment.
- Rapid onboarding of new stores.

MFT features and services 3

Managed File Transfer features and services include:

- Secure and reliable data movement
- Transport protocol support
- Participant management
- Flow management
- Ad hoc services
- Visibility
- Security services
- Centralized configuration and deployment

Secure and reliable data movement

Managed File Transfer enables the execution and management of data transfers within the enterprise or between the enterprise and its ecosystem, applications, and humans. These data transfers are executed either by a file transfer product, typically for internal transfers, or by SecureTransport acting as a routing hub between internal or external participants.

Data movement features include:

- Guaranteed delivery with file integrity checking, automatic retries, and checkpoint restart
- Flexible end-to-end acknowledgment
- Routing with protocol transformation
- Character transcoding
- Metadata accompanying the transferred file
- Transfer prioritization
- Bandwidth control
- File transfer acceleration

Transport protocol support

Managed File Transfer products allow you to transfer data using a variety of protocols:

- EDI-INT (AS1, AS2, AS3)
- FTP(S)
- HTTP(S)

- JMS
- OFTP
- PeSIT
- SFTP

For product protocol details, see *Data flows* on page 19.

Participant management

In Managed File Transfer, there are two types of participants:

- Business partners – Partners that exchange data with each other. Managed File Transfer provides complete partner management from the definition (contact information, technical details, certificates), to onboarding.
- Participants managing flows and middleware – A central service for identity and access management is provided mainly for the Transfer CFT configuration.

Flow management

The flow is the key concept of Managed File Transfer. It is the exchange of data between one or several participants. Each business interaction in transfer relies on the flow. A central flow repository is at the core of flow management. Flow definitions are stored in the repository and deployed to the systems involved. It is then possible to define a flow from an external partner to an internal application. This configuration is then deployed to the impacted middleware taking into account the potential conflict with existing flows.

Ad hoc services

Managed File Transfer enables human-to-human, human-to-system, and system-to-human interactions. People can send or receive files from a web UI, or email plug-in, as a file transfer or as an email with the file transferred as offloaded attachments. In any of these situations, the ad hoc files are transferred as securely and reliably as any other system-to-system transfer.

Visibility

Managed File Transfer provides visibility services with:

- End-to-end file tracking using the built-in tracking events generated by Axway 5 Suite or third-party products
- Defined alerts based on a particular set of events
- Web dashboards that provide flexible visibility options to meet the needs of different user roles

Security services

Managed File Transfer products provide the following security services:

- DMZ integration for data protection when interacting with external partners
- Data transfer security using SSL/TLS and file-level encryption
- Key and certificate management
- Data encryption during transport or at rest

Centralized configuration and deployment

Managed File Transfer provides centralized configuration and deployment for the file transfer engines.

Transfer CFT provides the following services:

- Operations – Start, stop, check status and apply update
- Technical configuration – Port, IP addresses, security
- Flow – Definition of flows which are deployed over all instances of Transfer CFT
- Application configuration – Definition of applications which are deployed over all instances of Transfer CFT

MFT products 4

Managed File Transfer is based on a flexible product architecture. Your choice of products depends on the services that you need to satisfy your business requirements. Your product portfolio can change as your business needs evolve.

The following diagram shows the portfolio of products in a Managed File Transfer implementation. Required products are typically used in all use cases, while the optional products play a role in certain business scenarios.

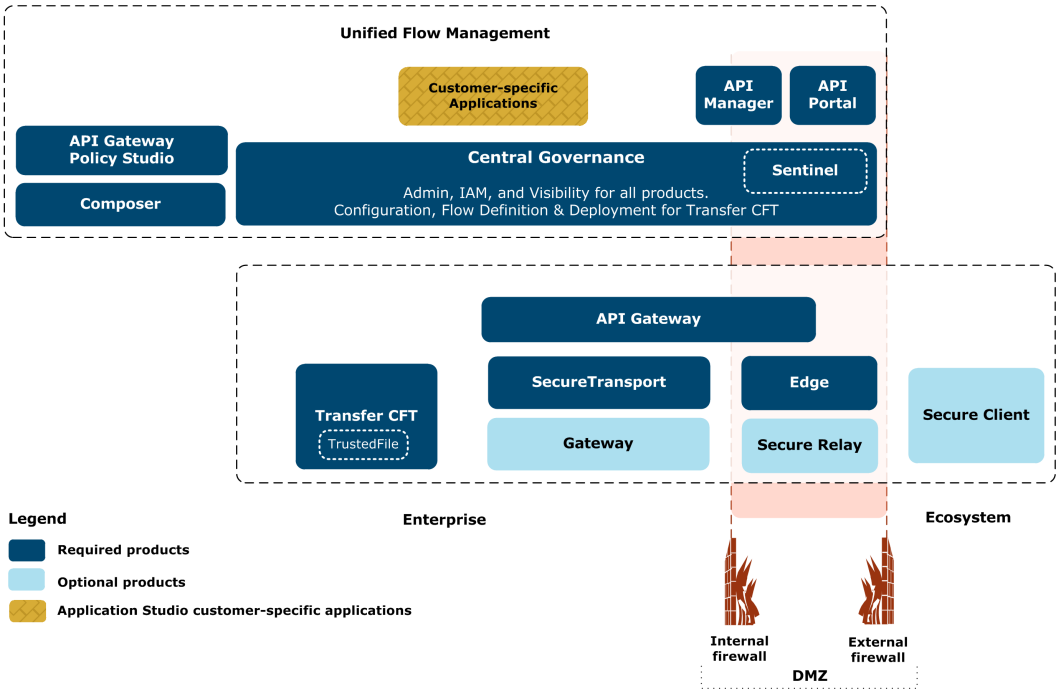

Figure 1. Product architecture

For descriptions of how the products interoperate, see *How the products work together* on page 18.

Required products

The following products are required:

- *Transfer CFT* on page 15
- *SecureTransport and SecureTransport Edge* on page 15
- *Central Governance* on page 15

- *Event Router* on page 16
- *API Gateway* on page 16

Transfer CFT

Transfer CFT is a transfer exchange controller that enables reliable and secure internal file transfers between applications. In Managed File Transfer, it can be used in a peer-to-peer, hub, or combination architecture. TrustedFile provides cryptographic features for encryption and digital signature. It is embedded in Transfer CFT and is used to secure data at rest.

SecureTransport and SecureTransport Edge

SecureTransport is an enhanced, secure, scalable, and highly available gateway for both system-to-system data transfers and ad hoc human transactions. In Managed File Transfer, SecureTransport is used as a hub to secure and route file transfers between partners and internal applications, and humans.

Using SecureTransport Edge, you can create a multi-tier file exchange infrastructure with multi-protocol managed file transfer, SSL termination, and back-end authorization that streams data across the DMZ to SecureTransport.

You can deploy multiple Edge gateways in the DMZ for load balancing and performance optimization.

SecureTransport Edge also safeguards compliance with SOX, GLBA, HIPAA, and other corporate, industry, and government mandates governing the security and privacy of sensitive information.

Central Governance

Central Governance provides a set of services for Axway 5 Suite products through a centralized interface. For all products, Central Governance provides Identity and Access Management (IAM) and visibility services. For Transfer CFT, Central Governance also provides product configuration, and flow definition and deployment services.

Central Governance provides the following key features for Transfer CFT:

- Global data flow repository, providing end-to-end data flow definitions, from business application to infrastructure level
- Automatic discovery of products to be managed
- Centralized management of product configuration and associated deployment, including mass processing capabilities for highly distributed environments, which include groups and configuration policies
- Centralized day-to-day operations management: to start and stop products and to view their logs

For IAM and security services, the Access and Security service provides:

- For Transfer CFT – Global management of user identity and rights and certificates, providing a central control point for security enforcement
- For other products – All native services are available via direct access to the services provided in Central Governance. These services include user management, certificate management, and security enforcement.

Note There will be two repositories for users: one for Central Governance and Transfer CFT and a separate one for the other products.

Note PassPort and Sentinel standalone are currently used to provide IAM and visibility services to the Accounting Integration products. However, Central Governance also provides these services through embedded editions of PassPort and Sentinel.

For IAM, the Access and Security service provides user management, certificate management, and security enforcement.

For Single Sign On (SSO) capability, an additional component is required: the SSO Agent.

For visibility, the Visibility service provides for all products:

- End-to-end centralized supervision of data flows, consistent with definitions in the repository
- Out-of-the-box alert management to track any problem linked to products or data flow processing, including a subscription mechanism for alert notifications
- Out-of-the-box web dashboards to get a global view of data flow activity, as well as the ability to create custom dashboards.

API Gateway

API Gateway is a comprehensive platform for managing, delivering, and securing enterprise APIs, applications, and consumers. In the context of Managed File Transfer, it can be used to manage APIs exposed by Transfer CFT, SecureTransport, or third-party products.

Event Router

Event Router is an additional component that provides the following functions:

- Event buffering – If the Central Governance Visibility service is unavailable, Event Router can buffer events from the product until it is available again.
- Throttling – Event Router can bundle events and send them in bursts, rather than one at a time.
- Routing – Event Router can direct events to a specific Central Governance server, enabling scaling.
- Filtering – Event Router can be configured so that unwanted events can be discarded and not sent to Central Governance.

Optional products

Secure Client

Secure Client is an MFT client that enables users to exchange files with the enterprise gateway in a secure and reliable manner. Designed for end-users, Secure Client provides protocol support for FTP (S), HTTP(S), and SFTP.

How the products work together 5

Managed File Transfer is a combination of Axway 5 Suite products that can transmit data securely from one or more sources to one or more destinations. Examples of these types of data exchanges include large CAD/CAM design files between manufacturing partners, commercial or legal documents, such as contracts or mortgage documents, and nightly product price updates from corporate headquarters to retail locations. The added value of Managed File Transfer resides in the governance of these data exchanges, from configuration to runtime monitoring and deployment on remote servers. Each of these steps are managed with consistent user experience in mind.

The following diagram illustrates how Managed File Transfer products work together to enable these types of file exchanges in an ecosystem that includes internal and external participants.

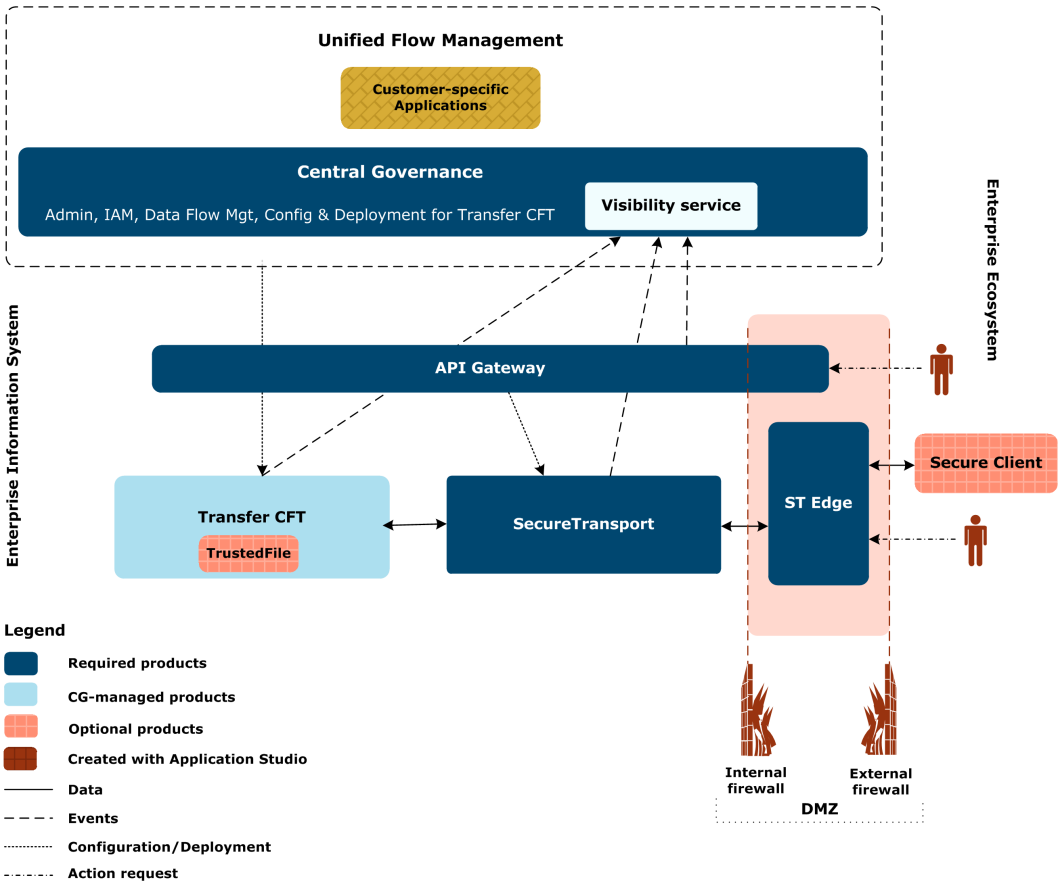

Figure 2. How the products work together

This diagram, which features SecureTransport as the communication gateway, illustrates how data, events, configuration information, and action requests are routed through the products in the reference solution.

Data flows

- File exchanges with external participants are routed through SecureTransport using SecureTransport Edge as the reverse proxy in the DMZ. Files received from external participants are routed to an internal application directly or through Transfer CFT. Internal data exchanges use Transfer CFT in either a distributed or centralized implementation. File sharing can be between external participants or a group of external participants. A file is sent from an external partner to SecureTransport through Edge. It is then made available for other external participants. For security reasons, the file is stored in the secured network and the external participant that wants to access it has to authenticate with SecureTransport Edge to be able to access the file.
- Exchanges initiated by an external participant through a web service call goes to API Gateway, which then routes the request appropriately.

Access management – Central Governance operates as a central repository to manage user access to products and to secure connections between products. SecureTransport handles access management itself. SecureTransport provides a delegated administration model. Through its access management system, a delegated administrator manages partners and the file exchanges that they process.

Visibility – Each product sends events to the Visibility service, which provides facilities to create dashboards, requests, and reports that afford end-to-end visibility on the data flows.

Configuration and deployment – Central Governance provides configuration and deployment services for Transfer CFT. Policy Studio is the configuration and deployment tool used with API Gateway. SecureTransport in a shared service model, delegates the administration of partners and flows to business users who want to manage their own ecosystem.

Data flows

This section focuses on the communication between the products that are involved in a data flow between an internal application and an external participant. A typical implementation involves:

- External participant – An external participant can be the initiator or the recipient of the exchange. It can be an application that is configured to trigger a transfer when it is necessary, or it can be a person who wants to interact with the back-end application through a portal or a client, such as Secure Client. When the external participant has large numbers of flows per day, it is advisable to use an application. Participants with a low number of flows per day should use Secure Client. For the participant with only a few flows per month, using a portal to upload data is most efficient.
- Communication gateway with DMZ integration – The communication gateway has two roles: It receives a connection request, validates it in the DMZ, and it then receives the data. Once the transfer is finished, it triggers the next action, which could be a transfer of the data to a back-end application through Transfer CFT. It can serve the same role for data coming from the back-end application that is being sent to an external participant.

- Transfer CFT – Provides final delivery, with encryption, to the back-end application, or serves as the first transfer monitor to be triggered by an application.

The following diagram shows an implementation using SecureTransport and lists the supported protocols. SecureTransport has its own set of supported protocols as listed in the table that follows the diagram.

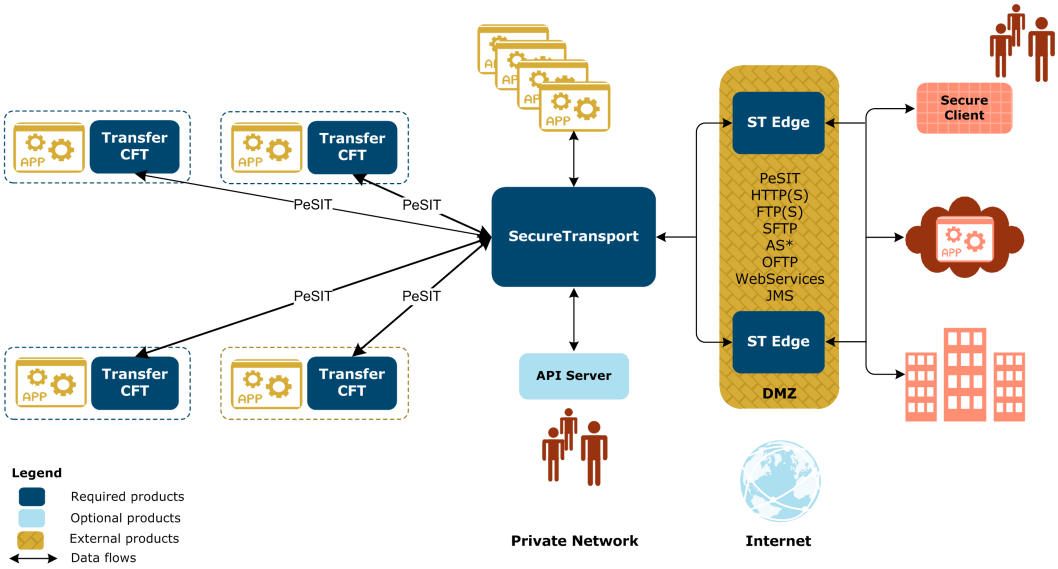

Figure 3. SecureTransport data flow protocols

In the following table, note that:

- AS*: SecureTransport is Drummond-certified.
- HTTP(S): SecureTransport can only connect to another SecureTransport for server-initiated transfers.

Protocol	SecureTransport
AS*	AS2
FTP(S)	Yes
HTTP(S)	Yes
JMS	No
OFTP	No
PeSIT	Yes
SFTP	Yes

The DMZ proxy that you use is also dependent on the communication gateway:

- SecureTransport uses Edge to provide protocol support outside of the DMZ. Edge manages the protocol session as well as the DMZ, and then transfers files in packets using a proprietary streaming protocol. Additionally, SecureTransport supports TLS termination and HSM.

Inbound flows

This section describes these types of inbound flows:

- From an external participant to a communication gateway
- From a communication gateway to Transfer CFT
- From a communication gateway to an application

From an external participant to a communication gateway

The connection between communication gateways and external participants is typically based on a business agreement and contains several SLAs. It is the responsibility of the communication gateway to store and apply this information. Each communication gateway has its own participant repository and manages the repository in its local database. To accept a connection request from an external participant, the communication gateway accesses this information.

For protocols with acknowledgment, the communication gateway triggers these once the file is received. It then updates initial transfer information to give visibility.

To be able to interact with the Internet, a communication gateway is integrated with the DMZ.

From a communication gateway to Transfer CFT

The communication gateway contains an engine that accesses the metadata of the incoming transfer and triggers a specific action. This action is typically to route the received file to an internal application via Transfer CFT. The configuration of this engine depends on the flow type and the final target of the file. To maintain a high level of flexibility for system integration, a routing accelerator should be added to the SecureTransport configuration. This accelerator is a custom addition to SecureTransport and requires implementation by Axway Professional Services.

From a communication gateway to an application

Based on metadata associated with the transfer, the communication gateway triggers certain payload routing actions to the internal applications. There are several ways to make a file available to an application:

- Drop the file in a given folder.
- Send the file to the application through protocols supported by the communication gateway.
- Send a notification to the application referencing the file that was deposited in a given folder.

Outbound flows

This section describes two types of outbound flows:

- From an application to the communication gateway
- From a communication gateway to an external participant

From an application to the communication gateway

An application can send files to a communication gateway targeting other participants in one of several ways:

- (Recommended method). The application sends a transfer request to Transfer CFT, which then sends the file using the PeSIT protocol to the communication gateway. PeSIT protocols can handle metadata that enable the communication gateway to determine the final destination of the file.
- Drop the file in a folder. The communication gateway can monitor the folder and trigger a transfer to the participant.
- Send a transfer request to the communication gateway referencing the path to the file that should be sent.
- Send the file through one of the communication gateway's supported protocols.

From a communication gateway to an external participant

The communication gateway can be a client that connects to a server hosted at the external participant. It then relies on the supported protocols to send the file. Alternatively, a file can be available in a folder and wait for the participant to connect to the communication gateway and download the file.

In either case, the communication gateway relies on DMZ integration.

Access management

Central Governance provides identity and access management services for most products comprising Managed File Transfer. SecureTransport is the primary exception.

When a user attempts an action requiring authorization (logging on for example), the product sends a request to Central Governance through the API. Central Governance approves or denies the request and responds so that the user can either perform the action, or is blocked.

Central Governance also provides a single sign-on (SSO) functionality that enables users to log on just once for all Central Governance services and for Transfer CFT.

The following diagram provides a high-level view of the use of Central Governance for user access.

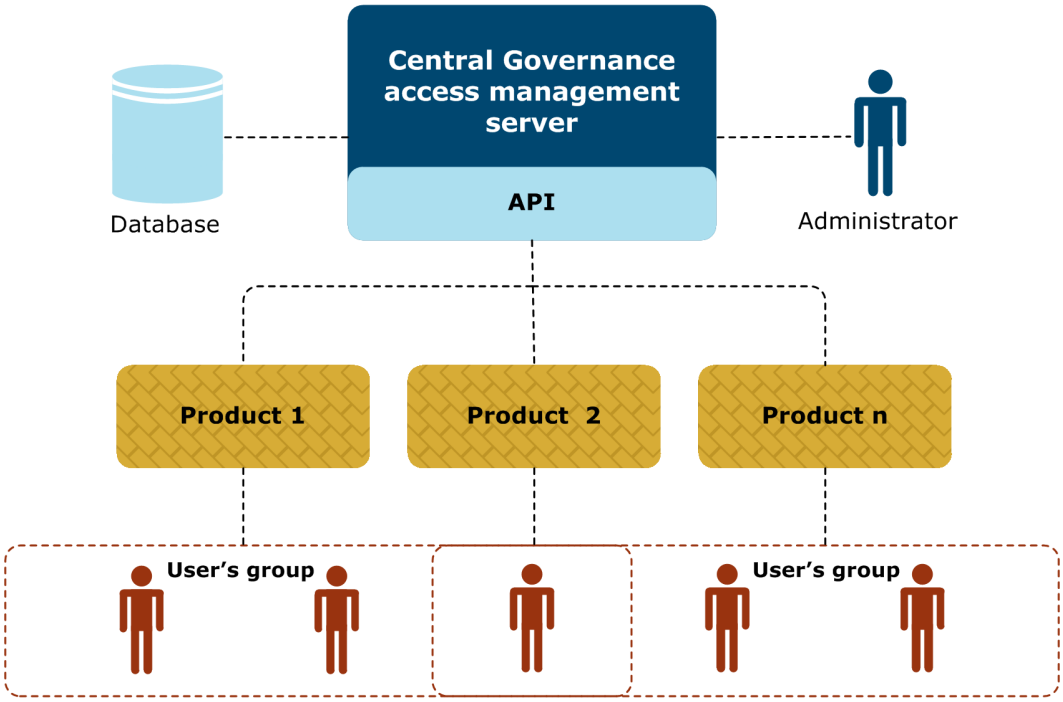

Figure 4. Access management overview

Visibility

The Central Governance Visibility service tracks technical, functional, and business events and shows them in an easy-to-understand way. It provides:

- Visibility – Optimizes processes and reduces problem resolution time and costs. It also enables you to drill down to the technical details to determine, for example, where an expected file is blocked or delayed.
- Intelligence – Aggregates business metrics with a correlation rules engine, and processes monitored data to define and initiate actions automatically.
- Traceability – Monitors all of your operations, including current and historical activity. It captures system-level changes as audit events and stores them for regulatory compliance. It also enables you to locate specific transactions using ascending and descending audit trail capabilities.
- Centralization – Provides a single, global view of your operations and business processes.

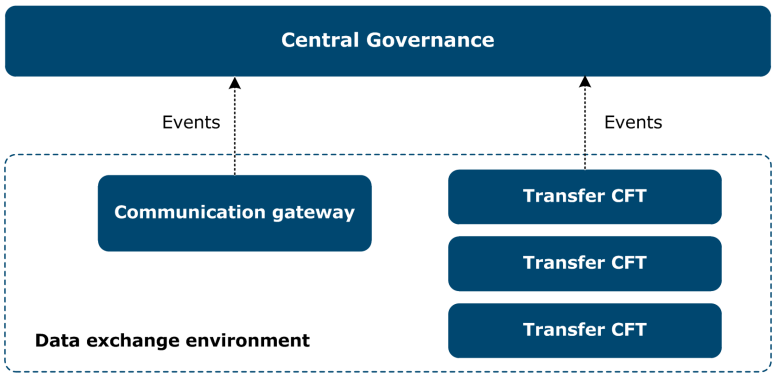

Figure 5. Visibility overview

Configuration and deployment

Central Governance is used to configure and deploy configurations to Transfer CFT systems individually and en masse through the use of configuration policies, which can be applied to multiple systems. It is also used to configure and deploy flows implemented by SecureTransport, or the different Transfer CFTs.

In the case of the shared service model, some administrative tasks are delegated to particular users who are in charge of their business unit (partner definition and flow definition). Those admin users connect to SecureTransport to execute their tasks.

Glossary

application programming interface (API)
A software program that facilitates interaction with other software programs.

communication gateway
A software program that manages the secure and reliable exchange of data between two or more points, often using the Internet.

data flow
The exchange of data between one or more source participants and one or more destination participants (sender/receiver).

decommission
Involves removal of a product, as well as the configuration changes that are required. For example, modifying data flow configurations that used the product. Decommissioning can also refer to the dismantling of the entire reference solution.

deployment
The process of sending a configuration from a design environment to the runtime environment. Also referred to as configuration deployment.

distributed exchange
A type of file exchange that is used exclusively for internal file transfer application integration.

DMZ
Demilitarized Zone. The virtual subnetwork, usually between firewalls, that performs a first level of control before granting access to the secure area when coming from an untrusted network. Highly secure architectures typically use two levels of DMZ, the public DMZ followed by the private DMZ.

DMZ proxies
Product or component designed to respect DMZ rules. DMZ proxies perform initial controls without any data storage on disk and avoid connections initiated in the DMZ.

document
A business document, such as an order, an invoice, or a payment, read in a data flow payload by the B2Bi Server or an Integrator Server. EDI transactions are typically documents.

dynamic integration process (DIP)
Represents the integration (typically data transformation or content-based routing) portion of a data flow. Dynamic in that a single integration process reads data flow content at runtime (from

metadata portion and/or actual payload) and, based on predefined profiles or agreements, and automatically executes the appropriate maps and custom modules. B2Bi DIP contains a set of predefined services (splitting, envelopping, duplicate detection, and so on) for the most popular B2B standards with a web UI exposing configuration options at runtime.

ecosystem
The extended enterprise, which includes the enterprise and its internal users, together with external parties, including subsidiaries, partners, customers, suppliers, and regulatory bodies with which it interacts.

edge
As in "the edge of the enterprise" - the boundary that divides the systems and users that are within and, therefore, controlled by the enterprise and the systems and partners that are external and outside of the scope of direct control of the enterprise. Typically, the edge of the enterprise is denoted by the DMZ, although this is changing with the increasing adoption of cloud services and the use of mobile applications.

enrollment
The first part of the onboarding process. Enrollment consists of the collection and review of relevant data from participants.

extension
An extension is an artifact that can be used to accelerate the time to value in a deployment. Extensions may be prepackaged artifacts, for example, scripts for FTP replacement, dashboards, dynamic integration processes, maps, process models, solution packs, forms, mail templates, libraries, detectors, envelopers, and so on.

gateway
See communication gateway.

implementation example
Diagram and description showing how the products in a reference solution can be used to solve an integration problem.

integration process
The integration portion of the data flow that corresponds to a sequence of map, custom stages (JMC or MBC) and/or prebuilt stages (detectors, splitters, enveloppers, and so on).

interaction
Represents an agreement between two parties that consists of the exchange of business information according to a service level agreement (SLA). Interactions involve the exchange of data, but can also include constraints on the exchange, such as a timeframe, or the manipulation of the data, such as enrichment. Interactions are conducted through data flows, which are themselves realized through the sequencing of data exchanges between middleware and products.

Managed File Transfer
A file transfer integration reference solution based on the Transfer CFT agent, managed by Central Governance. A Managed File Transfer reference solution includes a communication gateway.

map
A generic term for a step in the integration process that performs data transformation, payload parsing for visibility, content-based routing, data validation, or data enrichment. Maps can be expressed in various languages allowing the enterprise to maintain its assets (DML, DM, TFL, TF-XSL).

onboarding
The process by which required information related to a participant is collected and provided to the appropriate systems. Onboarding can be separated into two sub-processes: enrollment and provisioning.

participant
An entity taking part in business interactions. Participants can include applications, enterprises, communities and people inside and outside of an enterprise.

partner
A participant in an interaction. A partner can be an application, an enterprise, or a person. A type of participant that represents an internal organization, such as a business unit, or an external enterprise, such as a B2B trading partner.

promotion
The process of moving a runtime configuration from one environment to another. For example, from a test environment to a pre-production environment.

provisioning
The second part of the onboarding process. Provisioning involves the configuration of middleware. The participant information collected during the enrollment phase is used to configure gateways.

reference solution
A combination of Axway software products, components and extensions which, used together, solve an enterprise integration problem. These products may be installed in the customer data center or used as a service in the cloud.

Tracked Object
A model containing a set of attributes that describe an application event tracked by the Visibility service. Each incoming Tracked-Event Message contains a name field that indicates the name of the Tracked Object that is to be used with that message. Based on the implementation option, this Tracked Object can be persisted into a RDBMS table that exactly represents this Tracked Object data. Most implementations will persist the data.