SAP StreamWork

SECURE, COLLABORATIVE DECISION MAKING WITH SAP® STREAMWORK™

KEEP YOUR DATA SAFE AND PROMOTE EFFECTIVE COLLABORATION

THE BEST-RUN BUSINESSES RUN SAP™

CONTENT

4 Introduction

5 About Our Security
5 Personnel Access and Physical Security
5 Security Standards, Regulations, and Policies
5 Network Security
5 Application Security
6 Secure APIs
6 Confidentiality and Data Integrity
7 Availability

8 Maximizing Corporate Security
8 The Enterprise Agent in SAP StreamWork
8 Enterprise Agent Architecture
9 Web Administration Console
9 Enhanced Network Security
10 User Management
10 User Authentication
10 User Provisioning and Deprovisioning
11 Audit Reporting
11 Minimizing the Risk of Exposing Critical Information
11 For More Information

INTRODUCTION

SECURING INFORMATION IN SAP® STREAMWORK™

During the course of each business day, employees and contractors work, collaborate, and interact with colleagues, partners, and customers utilizing important and often sensitive information. At every juncture, information security is at risk, whether through dealings with internal stakeholders, during communications with external constituents, or through theft, damage, or malware. In spite of these risks, people both inside and outside the organization must be able to continuously work together, share information, and make informed decisions that lead to successful outcomes.

The SAP® StreamWork™ application is an on-demand collaborative decision-making application that enables companies to support flexible, collaborative work while addressing security requirements. SAP StreamWork brings together people, information, and proven business approaches to help teams drive successful results. Teams can organize, plan, develop strategies, collect feedback, and build consensus within a single software-as-a-service (SaaS) environment, thus improving the quality, timeliness, transparency, and repeatability of work and decisions. The application's open architecture allows organizations to take advantage of a secure, collaborative solution that integrates with SAP software and third-party enterprise applications – both in the cloud and behind corporate firewalls – to allow all team members to participate without fear of security breakdowns. Additionally, companies can securely deliver enterprise information via feeds or activity streams to business people and also develop their own business tools and integrations to support industry or line-of-business needs.

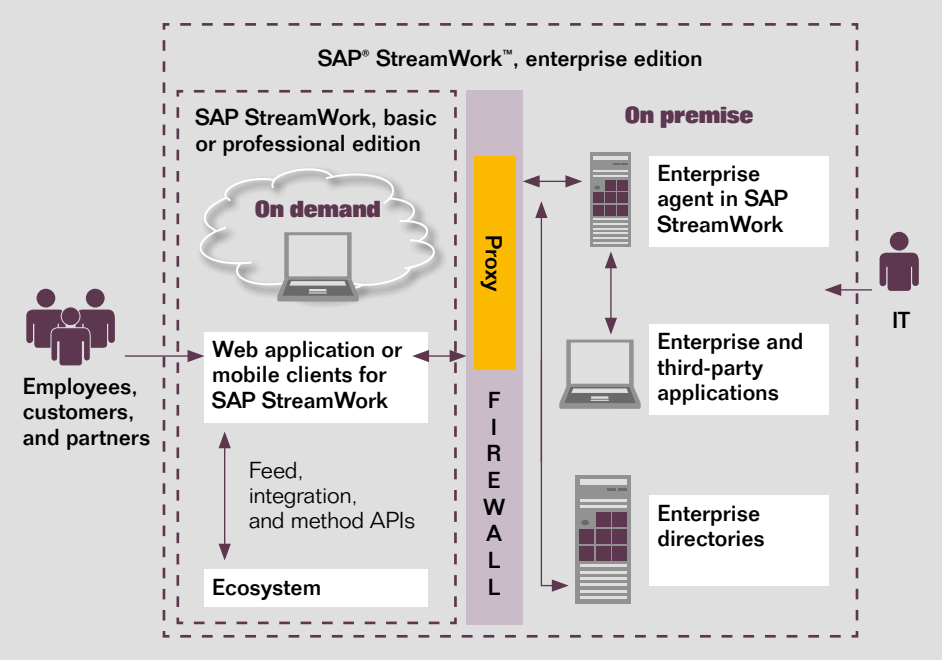

Figure 1: Teams Using SAP® StreamWork™ to Work Collaboratively Across Geographies

The SAP StreamWork application incorporates state-of-the-art security mechanisms and controls – including multiple firewalls, data encryption, and password protection – to help ensure critical information is highly secure yet still usable and shareable. Our security infrastructure is complemented by a simple and intuitive interface that enables users to maximize collaborative decision making within a secure and controlled environment.

The security infrastructure in SAP StreamWork is supported by:

- Experienced engineers and security specialists dedicated to round-the-clock data and systems protection
- Proven, up-to-date security technologies
- Ongoing assessment of emerging security developments and threats
- Complete redundancy throughout the entire online infrastructure of SAP StreamWork
- Total commitment to a secure, scalable, and reliable software system

SAP StreamWork is available in three different editions: basic, professional, and enterprise. This paper provides a brief overview of SAP StreamWork and describes the general security functionality and properties of the basic and professional editions. It then progresses to the enhanced security features available in the enterprise edition.

ABOUT OUR SECURITY

SAP GOES THE EXTRA MILE TO KEEP YOUR DATA SAFE

Personnel Access and Physical Security

Located in the United States and built to withstand worst-case disaster scenarios for every climate and locale, the data center for SAP StreamWork is protected by 24x7x365 surveillance, including motion-sensing, closed-circuit monitoring and recording; licensed on-site security staff; and secure card reader plus 4-digit PIN access to raised floor areas. Personnel must pass through electronic and visual identity validation systems and are subject to stringent authorization processes. The hosting facility maintains around-the-clock security guard coverage, including monitoring of all cameras, personnel access control, and alarm monitoring. Additionally, servers are securely situated inside locked cabinets with extremely restricted access.

Security Standards, Regulations, and Policies

The data center operations for SAP StreamWork are ISO 9001, ISO 20000, and ISO 27001 certified. ISO 9001 certification recognizes that an organization conforms to acceptable standards of quality at every stage of its product or service through a series of documented, repeatable processes. ISO 20000 certification addresses IT service management and recognizes processes for effective service delivery. The ISO 27001 security management standard establishes and maintains an effective information management system, using a continual improvement approach to govern the security of information and network systems. Further, the hosting operation undergoes an annual, independent SAS 70 Type II audit of logical, physical, and environmental controls.

Hosting services are strictly controlled by comprehensive policies covering security incident management, vulnerability alert management, patch management, account auditing, and new hires. All operations team members have signed special nondisclosure agreements with respect to the handling of customer data.

SAP StreamWork includes mechanisms to support the European Union's rigorous Data Protection Directive 95/46/EC on the processing of personal data within the EU. This directive constitutes the highest enforcement of privacy protection and human rights law in the world today. The hosting facility also complies with the U.S. Safe Harbor privacy principles, designed to prevent accidental information disclosure or loss.

Data center policies stipulate tight operating system–level security. The hosting team strengthens operating system security and hardens systems by disabling or removing any unnecessary accounts, protocols, and processes.

Vulnerability alerts trigger an automatic, repeatable, and documented response to prevent potentially significant damage to systems. The operations team evaluates every security alert that pertains to the infrastructure of SAP StreamWork and categorizes the risk according to a precise vulnerability alert management process. Threats to the hosting environment for SAP StreamWork are identified, categorized, and mitigated using multiple vulnerability alert services.

System patches are executed in accordance with clearly defined patch management and vulnerability alert management policies, using a risk-based approach to make sure that critical vulnerabilities are rapidly mitigated without putting production software in danger.

Network Security

To deliver a fault-tolerant, scalable environment, SAP uses a high-availability firewall architecture with hardware load balancers and standardized, hardened server builds. Advanced monitoring services sit on top of this architecture to quickly identify, diagnose, and remediate issues. The network perimeter is protected by multiple redundant firewalls and monitored by intrusion detection and intrusion prevention systems that provide physical and virtual identification and analysis of network traffic. Remote access to the network is restricted via two-factor authentication and segmented access rules.

Application Security

A valid username and password combination is required to access SAP StreamWork. User authentication details are encrypted via secure sockets layer (SSL) while in transmission. Any brute-force attempts to crack user passwords are mitigated by locking user accounts for extended periods of time after a given number of unsuccessful login attempts.

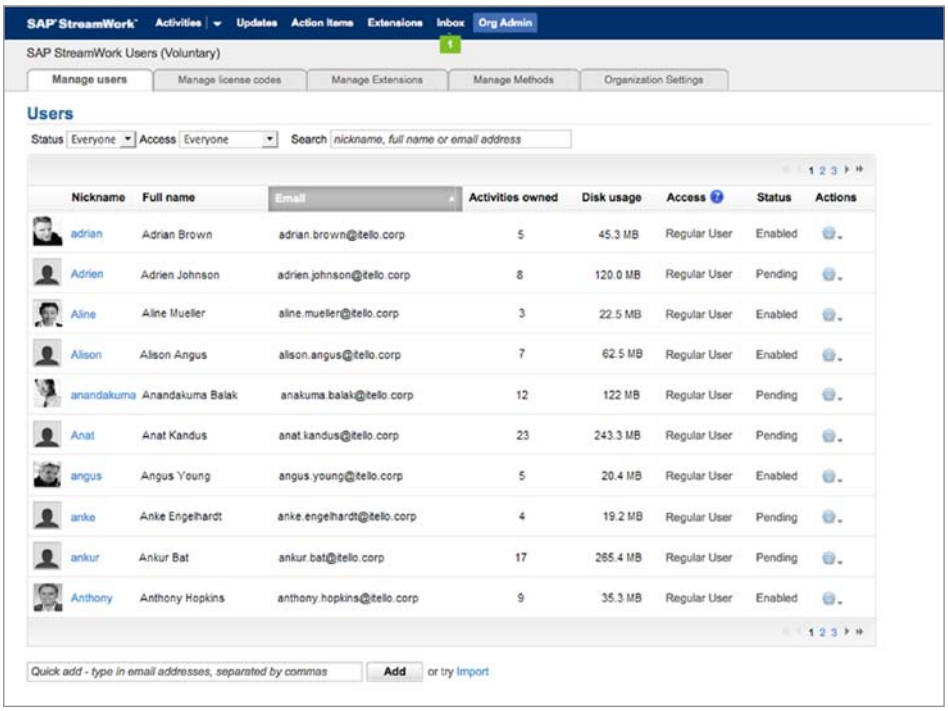

Figure 2: Organization Management Console in SAP® StreamWork™, Professional Edition

The robust application security model prevents SAP StreamWork users from accessing other users' data. Further, the architecture of SAP StreamWork guarantees that users can only access activities in SAP StreamWork that they have created themselves or to which they have been invited. As the activity owner, you can also disable other activity participants from inviting others to the activity. You can also create new activities from e-mails by forwarding threads to a unique e-mail address for SAP StreamWork. In this case, SAP StreamWork validates the authenticity of the e-mail sender to prevent any misuse.

Every document uploaded to SAP StreamWork is automatically scanned for viruses by an industry-standard virus scanner. Any infected file is immediately quarantined and cannot be shared among users.

An enhanced feature within the professional and enterprise editions of SAP StreamWork is the provision of an "organization." Organizations enable administrators to have added control over how SAP StreamWork can be used in your environment, simplifying user management and enablement and disablement of specific business methods and extensions. Activity owners can also make their activities "public," thus allowing the activities to become visible to other potential participants who can then request access (see Figure 2).

Secure APIs

SAP StreamWork also offers customers and partners application program interfaces (APIs) to further enhance and integrate with SAP StreamWork. The integration API is a Web service based on representational state transfer (REST) allowing Web, desktop, and mobile applications to connect to and interact with SAP StreamWork. This Web service API allows applications to interact with all objects in SAP StreamWork, including activities, feeds, and business methods. All APIs for SAP StreamWork require an authenticated user session. The APIs have the same level of access control as the user interface (UI) for SAP StreamWork. The application supports the following standard methods of user authentication for its APIs: OAuth, XAuth, and security assertion markup language (SAML). All API access of SAP StreamWork is audited using the same method as any standard access through the end-user UI.

Confidentiality and Data Integrity

SAP StreamWork secures your data using the strongest SSL and transport layer security (TLS) authentication and encryption products, including SSL certification during transmission. The padlock icon in the browser lets you know your data is fully shielded from unauthorized access while in transit.

Users can set e-mail notifications in SAP StreamWork to inform them of changes in activities and next steps. These e-mail notifications are also fully encrypted if the receiving e-mail server supports TLS encryption.

Customer data is stored on high-performance, low-latency enterprise-class servers with solid-state drives and multiple data paths for redundancy and fault tolerance. Data hosted on SAP StreamWork is protected against loss by a robust backup process, and the resulting backup is again encrypted when sent off-site.

The partner ecosystem for SAP StreamWork offers additional, complementary third-party integrations and extensions. If users opt to use third-party extensions within SAP StreamWork, they will typically need to register for the partner service and accept the terms and conditions. In this case, content in SAP StreamWork may be stored by the partner service and is subject to the security provisions delivered by that service. In the professional and enterprise editions of SAP StreamWork, administrators can restrict the use of extensions in an organization.

Availability

SAP StreamWork delivers industry-leading service with high availability and uptime. The service-level agreement with our operations team defines a minimum network availability of 99.95%. Platform availability (hardware, operating system, and physical storage) is fault-tolerant to 99.99%.

Data center monitoring is ongoing 24x7x365, including fault, performance, and transaction monitoring. Within these areas, the operations team deploys a number of different monitors to provide the necessary information and response. Redundant electrical generators, redundant cooling systems, and backup equipment support the production equipment to help ensure servers are continually up and running.

At SAP, ensuring the security of your information is a number one priority. The SAP StreamWork application incorporates state-of-the-art security mechanisms and controls complemented by a simple and intuitive interface that enables users to maximize collaborative decision making within a secure and controlled environment.

MAXIMIZING CORPORATE SECURITY
USING SAP STREAMWORK, ENTERPRISE EDITION

SaaS enterprise applications are taking the world by storm and represent a fundamental shift in how software solutions can be deployed and managed. However, some enterprise IT departments are still hesitant to adopt SaaS applications due to concerns around corporate integration, visibility, and control.

To overcome these concerns, the enterprise edition of SAP StreamWork leverages proven Novell technology to provide an on-premise enterprise agent that securely delivers key IT features, such as user provisioning and deprovisioning from enterprise directories, single sign-on, and auditing of user events.

The Enterprise Agent in SAP StreamWork

The enterprise edition of SAP StreamWork leverages SUSE Linux Enterprise Server and SUSE Appliance Toolkit from Novell to deliver the enterprise agent in SAP StreamWork. The enterprise agent is a virtual appliance that securely integrates the cloud-based application with a company's on-premise business system. To further enhance security requirements and simplify administration, the underlying SUSE operating system has been customized to disable all functionalities that aren't needed when running the enterprise agent.

All applications in the enterprise agent virtual image have been securely configured. As the virtual appliance also includes an automatic software update mechanism, any security vulnerabilities of included applications can be immediately fixed through deployment of the latest security patches. You can manage updates for your deployment by scheduling automatic update checks and selecting a date, time, and recurrence to install downloaded updates. The enterprise agent also lets you back up your system settings into a data file for future restoration on a new system.

The enterprise agent runs periodic checks in the event of root access to the system or if settings are changed. In this eventuality, an error message is sent to the enterprise agent administrator, and the agent's activities are shut down until it has been reset to the default settings or the last validated configuration.

Enterprise Agent Architecture

During installation, the enterprise edition of SAP StreamWork installs and configures two components: the enterprise agent and the Web administration console. The enterprise agent is generally deployed behind the customer's DMZ firewall (see Figure 3).

The enterprise agent in SAP StreamWork connects to the following existing components in your enterprise:

- Enterprise directory
- Reverse proxy server
- Proxy server (optional)

Through your enterprise directory, you can map your user groups to the enterprise agent and enable users to log into SAP StreamWork with their enterprise user name and password. The enterprise agent currently supports Microsoft

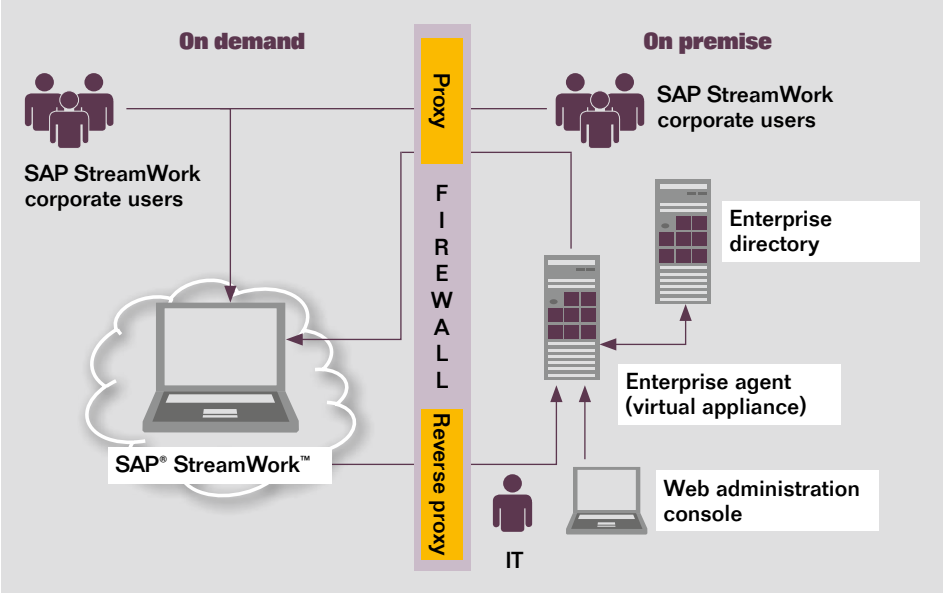

Figure 3: Architectural Overview of the Enterprise Agent in SAP StreamWork

Windows Active Directory and custom lightweight directory access protocol (LDAP) v3–compliant directory services as enterprise directories.

Reverse proxy servers protect internal servers from external networks by receiving requests for internal resources and proxying those requests onto the relevant machines internally. A reverse proxy in the DMZ firewall allows inbound connections from SAP StreamWork to your corporate network and redirects information received from SAP StreamWork to the machine containing the enterprise agent. The enterprise agent also supports the use of an outbound proxy server if your corporate network requires one for Internet access.

Web Administration Console

The Web administration console is a Web-based tool for administrative tasks, such as user provisioning, certificate management, registration, and server management. Administrative access to the enterprise agent in SAP StreamWork takes place only through the Web administration console (see Figure 4).

Access to the enterprise agent Web administration console requires user and password authentication. The enterprise edition requires the administrator to change the password after installation, automatically checks and displays the password strengths, and only accepts strong passwords. To thwart brute-force attacks against the administrator password, the administrator account is locked for an extended time after a specified number of unsuccessful login attempts.

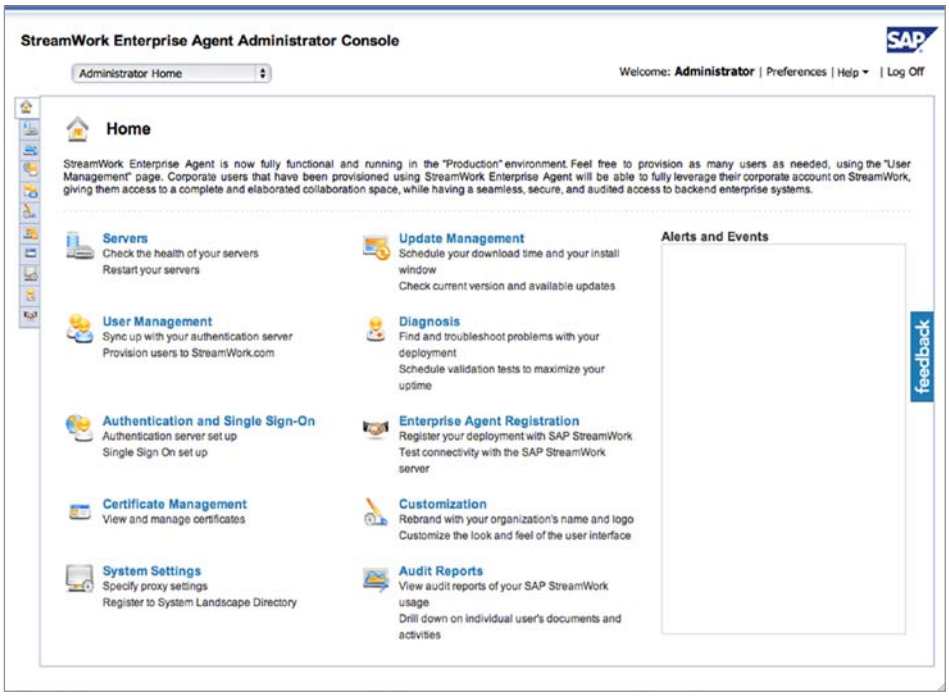

Figure 4: Enterprise Agency Administrator Console Home Page in SAP® StreamWork™

Enhanced Network Security

Your network infrastructure is extremely important in protecting your system. Your network must support the communication necessary for your business needs without allowing unauthorized access. A well-defined network topology can eliminate many security threats based on software flaws (at both the

With the enterprise agent Web administration console in the SAP StreamWork application, administrators can:

- Specify the enterprise directory servers to use for authentication and the user groups authorized to use SAP StreamWork
- Transfer content between authorized users of SAP StreamWork
- Specify the time of day when available updates are checked for and downloaded
- Specify whether updates are to be applied automatically or manually
- Specify the time period to apply updates (if automatic updating is enabled)
- Apply an update (if manual updating is enabled)
- Roll back an update

operating system and application level) or network attacks such as eavesdropping. If users cannot log on to your application or database servers at the operating system or database layer, then there is no way for intruders to compromise the machines and gain access to the back-end system's database or files. Additionally, if users are not able to connect to the server LAN, they cannot exploit well-known bugs and security holes in network services on the server machines.

SAP recommends installing the enterprise agent for SAP StreamWork inside the corporate firewall and having a reverse proxy URL set up in a DMZ. From a purely technical point of view, the enterprise agent could also be deployed in a corporate environment where no DMZ exists.

To minimize vulnerability risks, the enterprise agent only allows network access through a few well-documented network ports, which can be readily monitored and further secured through an encrypted HTTPS connection. Internally, the enterprise agent uses only one specific port to connect to the corporate directory. All communication with the enterprise directory is SSL-encrypted.

The enterprise agent includes a default certificate that is self-signed. This certificate is used when users are logging in to SAP StreamWork. It is recommended that you replace the default certificate with a third-party signed certificate.

User Management

Important aspects of user management are authentication and provisioning and deprovisioning.

User Authentication

Authentication is the process of verifying the identity of a user who attempts to access the system. Authorization is the process of verifying that the user has been granted sufficient rights to perform the requested action upon the specified object. The methods of authentication that the enterprise agent in SAP StreamWork currently supports are Microsoft Windows Active Directory with Kerberos and custom LDAP v3–compliant directory services. This section provides an overview of how authentication works within the enterprise agent.

During initial setup of the enterprise agent in the corporate infrastructure, a unique SAML certificate is generated based on the customer's organization and the initial licensing key. This certificate establishes a trusted relationship between the enterprise agent and SAP StreamWork.

Users of the enterprise edition of SAP StreamWork can log in using their corporate credentials. This data is never saved on SAP StreamWork. The login information is redirected to the corporate user directory for authentication.

The enterprise agent also supports single sign-on (SSO) in conjunction with Microsoft Windows Active Directory and Kerberos. When you enable SSO settings, provisioned users do not need to enter their enterprise credentials to log onto SAP StreamWork while accessing the application from inside the corporate firewall. The credentials you specify are used to process SSO to SAP StreamWork through the enterprise agent. For security reasons, SSO tickets are generally valid only for a very short time span.

To enable SSO from a Web browser, you must enable Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO). SPNEGO is a protocol used to implement SSO solutions. It is used when a client application wants to authenticate to a remote server, but neither end is sure what authentication protocols the other supports.

User Provisioning and Deprovisioning

The enterprise agent in SAP StreamWork allows customers to fully automate the provisioning and exclusion of user access for the application. Users do not need to individually register for SAP StreamWork; administrators have full control over access for individuals, groups, and departments for quick, simple deployment. In addition, the enterprise agent also enables corporate customers to remove corporate users of SAP StreamWork from the application and transfer their content to new owners, in cases such as when employees change roles or leave the company.

The enterprise agent connects to the enterprise directory to retrieve a list of users who are members of groups authorized to use SAP StreamWork. This

list of e-mail addresses – without user ID or password information – is sent to SAP StreamWork to create user accounts.

In the enterprise agent, administrators can readily configure the enterprise directory groups to receive access to SAP StreamWork. The enterprise agent schedules daily jobs to sync the enterprise users and user group information. In the case of new corporate users, the enterprise agent notifies SAP StreamWork, and the system automatically sends invitation e-mails to activate their new accounts in the application. Users will be authenticated through standard enterprise agent procedures prior to actual activation.

Users removed from the specific enterprise directory groups are also disabled from SAP StreamWork. The enterprise agent periodically updates user and user group information and notifies SAP StreamWork of any disabled users. It also executes real-time enterprise directory queries to ensure user rights during login to SAP StreamWork from outside the corporate firewall and to block disabled users. Enterprise administrators can then reassign ownerships of any disabled user's published content in SAP StreamWork to other users.

Audit Reporting

The enterprise agent in SAP StreamWork includes comprehensive audit reporting functionality to help support customers' auditing requirements. The audit information is encrypted in the enterprise agent audit database and stored behind the corporate firewall. Prebuilt reports are ready to run and contain information on:

- Content uploads by users – for example, are they uploading sensitive content into shared activities?
- Participants in activities in SAP StreamWork – for example, are they internal or external users?
- What is happening within activities – for example, what are the most edited or the most viewed activities?
- System configuration changes and issues – for example, who made a specific change to the system?

Minimizing the Risk of Exposing Critical Information

Organizations can gain significant competitive advantages through effective and secure collaboration. SAP StreamWork enables companies to make better use of people and information assets while minimizing the risk of exposing critical information. The software employs multiple layers of security to allow users to safely and securely collaborate and share their data with customers, partners, and suppliers. With SAP StreamWork, your data is safe from unwanted intrusion or accidental exposure within an infrastructure you can trust. The enterprise edition of SAP StreamWork further extends security features in the application to fully support corporate requirements such as network security protocols, user provisioning and deprovisioning, single sign-on, and auditing capabilities.

The data center operations for SAP StreamWork are ISO 9001, ISO 20000, and ISO 27001 certified. Hosting services are strictly controlled by comprehensive policies and undergo an annual, independent SAS 70 Type II audit of logical, physical, and environmental controls.

For More Information

To learn more about how SAP StreamWork can transform the way decision making works at your organization, please visit www.sapstreamwork.com or contact your SAP representative.

50 103 960 (11/03)
©2011 SAP AG. All rights reserved.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase, Inc. Sybase is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

www.sap.com/contactsap

THE BEST-RUN BUSINESSES RUN SAP™