A PRODUCT OVERVIEW
SUN™ SECURE GLOBAL DESKTOP SOFTWARE

White Paper
March 2006

Table of Contents

About Sun™ Secure Global Desktop Software

Sun™ Secure Global Desktop Software provides secure access to server-based applications running on Microsoft Windows, Solaris™ Operating System, Linux and other UNIX®, Mainframe and Midrange systems from a wide variety of popular desktop PCs and mobile devices. Utilizing a unique three-tier architecture, the software delivers modern desktop applications side by side with legacy applications without costly modifications to existing software. This allows for consolidation of critical applications and data onto highly reliable, centrally maintained servers and off individual desktop and laptop computers, improving manageability while increasing flexibility.

“Centralization” is a key concept in Sun Secure Global Desktop Software. Architecturally, the software provides a framework upon which to build a centralized computing model. By centralizing corporate assets in the form of computer resources, applications, and data, these items can be better controlled, protected, and more fully utilized. Centralizing intellectual property, whether in the form of computer code, business intelligence, or proprietary or confidential information, allows for better control, better accuracy, and better protection, than the alternative of allowing it to be distributed and copied in an uncontrolled manner among dispersed computers and users. At the same time, centralization can substantially reduce administrative overhead by removing complex and troublesome software from difficult to manage client devices and placing it instead on centrally managed servers.

Sun Secure Global Desktop Software allows organizations to quickly realize the benefits of Web-enabled application delivery; speed of applications deployment, reduced client complexity, reduced administrative costs, and better control and accuracy of business data.

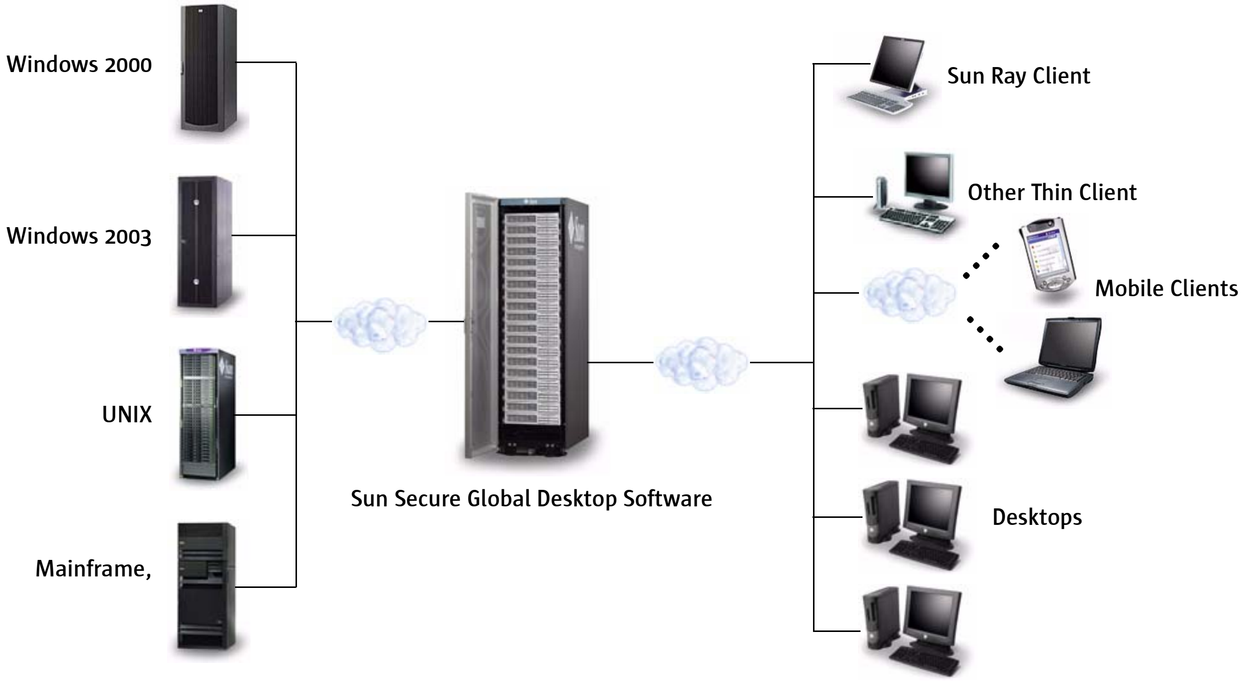


Figure 1. Sun Secure Global Desktop Software Architecture Diagram

With Sun Secure Global Desktop Software, users access applications remotely from their client device. Users need only a Java™ technology-enabled Web browser (such as Mozilla™ Firefox). This approach:

- Allows application access from the corporate internet or over the public internet safely and securely.
- Ensures users can access only the applications they're authorized to use.
- Centralizes management of users, applications, and data.
- Enables auditing of application usage.
- Eliminates the need to install software packages on each client device.
- Dramatically reduces the time to deliver applications.
- Allows users to have a consistent work experience, whether in the office, at home, or on the road.

Sun Secure Global Desktop Software uses an innovative architecture that integrates diverse application types, and diverse client devices, with little or no disruption to the existing IT environment.

- Applications continue to run untouched on existing application tier servers.
- Client devices such as Microsoft Windows PCs, Solaris or Linux workstations, Apple Macintosh computers, thin clients, and mobile devices can all be used.
- A wide range of connection types are supported, and the Adaptive Internet Protocol (AIP) ensures optimal performance over the most challenging network environments, including network connections with limited bandwidth, and/or high latency, and adapts itself to the current network environment; a sudden increase in latency or change in network bandwidth is automatically detected by the AIP protocol, and it adapts its strategies to this ever-changing environment to ensure optimal application performance.

Sun Secure Global Desktop Software is installed on one or more dedicated Solaris or Linux servers, centrally storing a wide range of information about the users and their applications. To access their applications, users browse to a URL with a Java technology-enabled Web browser and enter their authentication information. This authentication procedure optionally ties to an organization's existing Identification and Authentication mechanism—for example, an organization's existing LDAP or Active Directory directory service can be used as the authentication authority in Sun Secure Global Desktop Software. Such a service is called a "Login Authority" in Sun Secure Global Desktop Software terminology.

Once authenticated, the Sun Secure Global Desktop Software server checks its datastore of users and application information to determine which applications each user is authorized to access. This dynamically generated set of applications is then presented to the user in the form of a "webtop", a Web-based desktop showing icons and URL links for each permitted application. At all times, Sun Secure Global Desktop Software manages connections, user sessions, and security, providing a record of all actions.

Sun Secure Global Desktop Software is designed as a modular, scalable, and flexible solution. It is ideally suited for use by data centers of all types, including Application Service Providers (ASPs) and other service providers that need to deploy a mix of applications to large numbers of geographically dispersed users with a range of client devices and connectivity types.

Architecture by Example

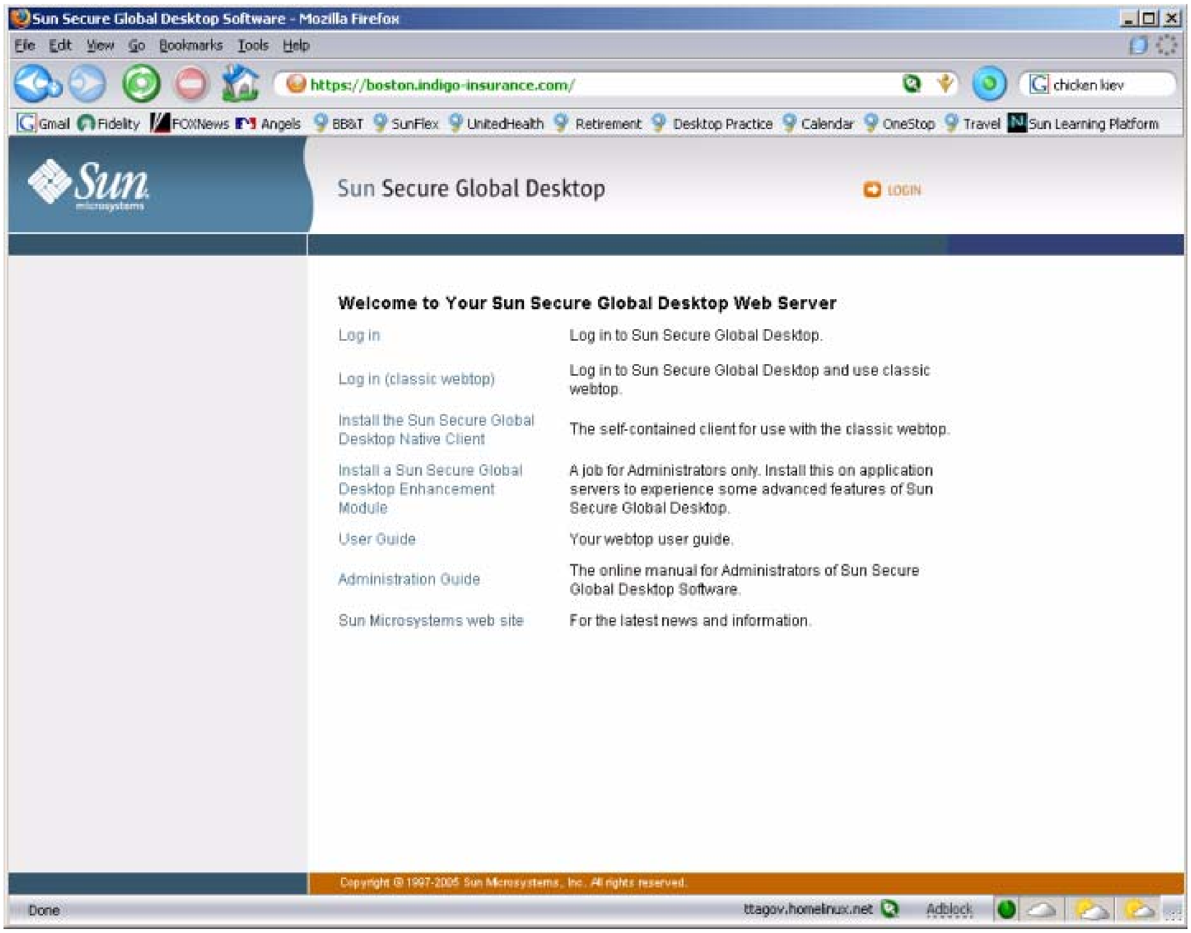
This section presents an overview of the Sun Secure Global Desktop Software architecture by describing what happens when an employee of Indigo Insurance, a fictitious organization, logs in and starts an application.

Some terminology is introduced in this section. When you read later parts of this white paper you may want to refer back here for an overview or to the glossary at the end.

Users can access Sun Secure Global Desktop Software from a Web browser or by using a Sun Secure Global Desktop Native Client. The process is similar for both cases. In our example we'll follow a Web browser user.

Secure Access

Elizabeth Blue starts her Web browser and types the URL for a corporate Sun Secure Global Desktop Software Server: `boston.indigo-insurance.com`. Her Web browser makes a secure connection to the Web server, ensuring the integrity and privacy of data sent between the Web browser and Web server. A Web page is displayed in Elizabeth's browser, similar to the following:


Sun Secure Global Desktop Software - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://boston.indigo-insurance.com/
chicken kiev
Gmail Fidelity FOXNews Angels BB&T SunFlex UnitedHealth Retirement Desktop Practice Calendar OneStop Travel Sun Learning Platform
Sun microsystems
Sun Secure Global Desktop
LOGIN
Done
ttagov.homelinux.net
Adblock

Welcome to Your Sun Secure Global Desktop Web Server

Log in	Log in to Sun Secure Global Desktop.
Log in (classic webtop)	Log in to Sun Secure Global Desktop and use classic webtop.
Install the Sun Secure Global Desktop Native Client	The self-contained client for use with the classic webtop.
Install a Sun Secure Global Desktop Enhancement Module	A job for Administrators only. Install this on application servers to experience some advanced features of Sun Secure Global Desktop.
User Guide	Your webtop user guide.
Administration Guide	The online manual for Administrators of Sun Secure Global Desktop Software.
Sun Microsystems web site	For the latest news and information.

Copyright © 1997-2005 Sun Microsystems, Inc. All rights reserved.

Figure 2. Sun Secure Global Desktop Software Welcome Page

This Web page provides links to various tools and resources, including links for logging in to the Sun Secure Global Desktop Software server.

When Elizabeth clicks on the “Log in” link, the first thing that occurs is that the Sun Secure Global Desktop Software server checks to ensure that the proper version of the Sun Secure Global Desktop Software client component is installed on her machine. If the client component is not available, it is automatically transferred to her machine from the server.

This client component is required to communicate with a Sun Secure Global Desktop Software server, encoding and decoding the AIP protocol, launching and displaying applications, encrypting/decrypting Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections, and many other functions. There are three major client types used in conjunction with Sun Secure Global Desktop Software; see “Chapter 9: Client Support” for more information.

Once downloaded, the client will remain on her computer until a new version is available. If she moves to another computer, then the process is simply repeated on the new machine. Once it is determined that the latest client component is available, it is launched and a login form is displayed in the Web browser.

Flexible Authentication

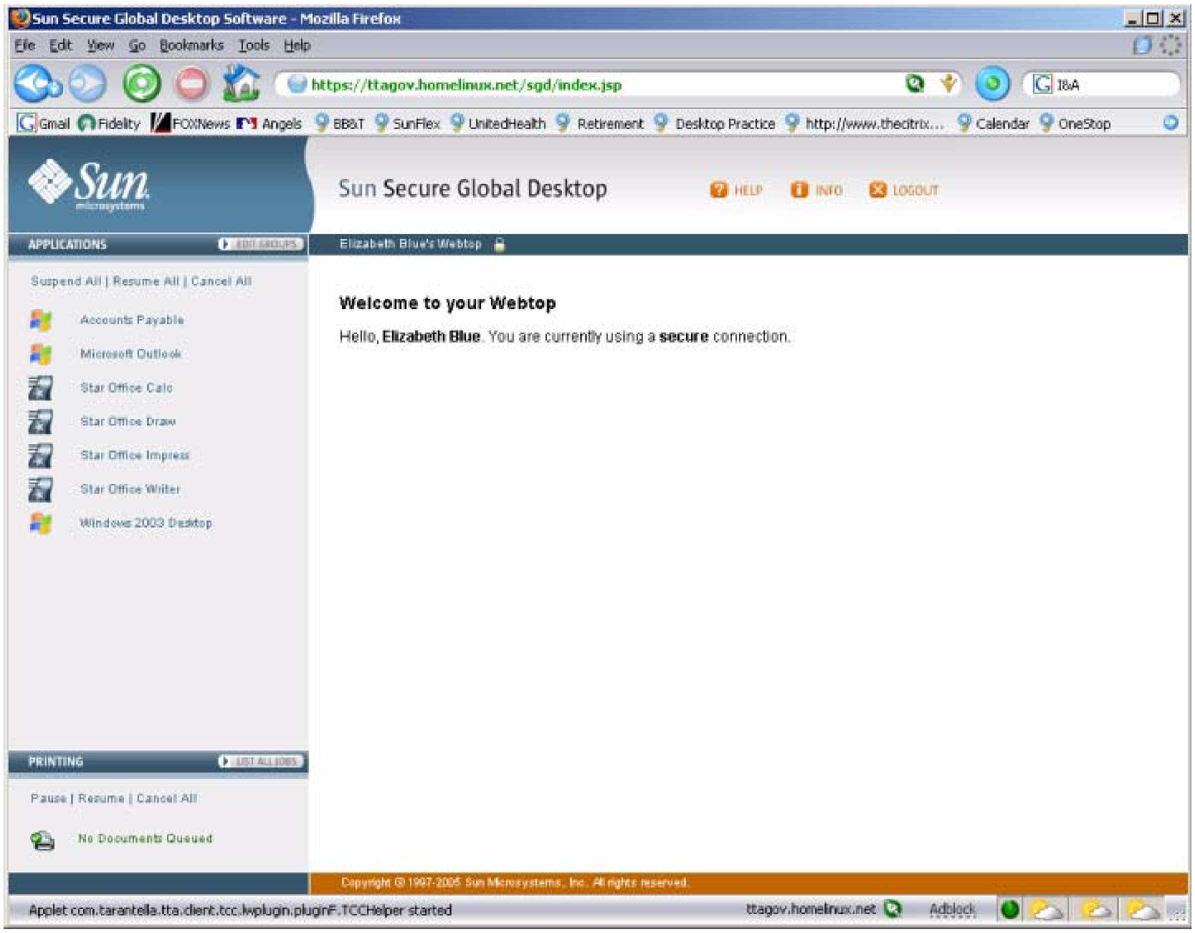
Now that the connection is established with the server and the client component is launched, Elizabeth can type her authentication credentials into the User name and Password text boxes and click Log In. Her credentials are passed to the Sun Secure Global Desktop Software server and checked against the configured authentication services, which may include an LDAP directory, a Microsoft Windows NT/2000 domain, a Microsoft Active Directory Catalog Server, an RSA ACE/Server for SecurID authentication, or a UNIX password database.

Sun Secure Global Desktop Software can also integrate with Web server (HTTP) authentication, allowing users who have already logged in to a Web server to bypass the Sun Secure Global Desktop Software login prompt and login directly. This feature is called “Web server authentication”.

Note that Secure Global Desktop doesn't necessarily introduce another username and password for users to remember. Integrating with industry standard identity and authentication mechanisms allows for a simplified experience, utilizing the same credentials that are used on other systems.

Once authenticated, the Sun Secure Global Desktop Software server determines the content of Elizabeth's Webtop; that is, what applications she is entitled to run. It may also determine whether she should be given a secure connection, based on the location from where she is connecting. For example, Elizabeth might be configured to use a secure connection when accessing the Sun Secure Global Desktop Software Server across the Internet, and a standard connection when located within the corporate intranet.

Finally the Web browser displays the Webtop, a Web page which includes an application launch bar, which lists the applications Elizabeth is allowed to run, as shown below:


Sun Secure Global Desktop Software - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ttagov.homelinux.net/sgd/index.jsp
I&A
Gmail Fidelity FOXNews Angels BB&T SunFlex UnitedHealth Retirement Desktop Practice http://www.thecitrix... Calendar OneStop
Sun microsystems
Sun Secure Global Desktop
HELP
INFO
LOGOUT
APPLICATIONS
EDIT GROUPS
Elizabeth Blue's Webtop
Suspend All | Resume All | Cancel All
Accounts Payable
Microsoft Outlook
Star Office Calc
Star Office Draw
Star Office Impress
Star Office Writer
Windows 2003 Desktop
PRINTING
LIST ALL JOBS
Pause | Resume | Cancel All
No Documents Queued
Copyright © 1997-2005 Sun Microsystems, Inc. All rights reserved.
ttagov.homelinux.net
Adblock

Welcome to your Webtop

Hello, **Elizabeth Blue**. You are currently using a **secure** connection.

Applet com.tarantella.tta.client.tcc.lwplugin.pluginF.TCCHelper started

Figure 3. Sun Secure Global Desktop Software Webtop

From this Web page, Elizabeth can start new copies of applications, "resume" applications that she suspended in previous sessions, terminate running application instances, control print jobs, and so on. She can also customize the display to her liking, by organizing her applications into groups, and she can either bookmark or drag and drop application shortcuts from her Web page onto her desktop to enable quick access to those applications in the future.

Multiple Application Types

In Sun Secure Global Desktop Software, applications run unchanged on application tier servers, client devices display the applications to users, and Sun Secure Global Desktop Software servers broker connections between them, creating a three-tier architecture. Client devices and application tier servers connect only to Sun Secure Global Desktop Software servers, never to each other. This "shield" protecting the critical application tier servers is an important aspect of the security and control provided by Sun Secure Global Desktop Software.

The three-tier architecture allows Sun Secure Global Desktop Software to support many different types of applications without requiring additional client software or application tier server software. The Sun Secure Global Desktop Software server handles the details of each application type, ensuring that a single protocol is used to client devices. This protocol, the Adaptive Internet Protocol, is covered in more detail later. Its job is to optimize the user experience so applications feel to end users like they are executing on their local client devices.

Whatever the type of application, Elizabeth can just click its icon on her Webtop and a few seconds later it is displayed on her client device. Application visualization is performed by a Display Engine on her client device, provided by the client component. This Display Engine receives display updates from and sends user input to a corresponding Protocol Engine running on an Sun Secure Global Desktop Software server. Protocol Engines are responsible for communicating, in turn, with application tier servers using the appropriate native protocols, such as RDP, X11 or VT100—in effect, acting as a server-side client. If Elizabeth has a secure connection, traffic between Display Engines and Protocol Engines is encrypted.

When Elizabeth clicks an application's icon, the client component starts a Display Engine, which sends a launch request to the Sun Secure Global Desktop Software server. The request arrives at either the SSL Daemon or Sun Secure Global Desktop Software Proxy Server components, depending on whether Elizabeth's connection is secure or not. The Sun Secure Global Desktop Software Proxy Server and SSL Daemon perform similar roles, handling and routing connections to the appropriate processes on the Sun Secure Global Desktop Software server. The SSL Daemon encrypts and decrypts traffic to and from client devices to ensure data privacy and integrity.

Whether Elizabeth's connection is secure or not, the launch request is passed to the JServer component of the Sun Secure Global Desktop Software server. The JServer is the decision-making process, maintaining and controlling access to configuration and database information and handling tasks such as user authentication, application launch and resumption, data replication, load balancing and session management.

The JServer initiates a launch through the Protocol Engine Manager, which does two things:

- Starts an Execution Protocol Engine. This connects to the application tier server, logs in as the appropriate user, sets some environment variables as needed, and then executes the application. If Elizabeth’s password for the application tier server (or domain) is not stored in the secure password cache, this is fed back to the Display Engine, which prompts her for the appropriate credentials.
- Starts a Protocol Engine appropriate to the type of application: either a Graphics Protocol Engine (used for X11 or Microsoft Windows applications) or a Character Protocol Engine. The protocol engines use the requested application’s native protocol (such as X11 or RDP) to communicate with the application tier server, and Adaptive Internet Protocol (AIP) to the Display Engine to communicate with the client device.

Scalability, Redundancy and Load Balancing

A single Sun Secure Global Desktop Software server can support several hundred concurrent users (depending on system specifications). To support several thousand concurrent users, several servers can be joined together to form an array. Managing an array is very similar to managing a single server; in most cases you can think of the array as a single entity rather than a collection of servers.

As far as Elizabeth is concerned, all array members are equivalent. Whichever array member Elizabeth logs in to, she sees the same applications on her Webtop.

When Elizabeth starts an application, the associated Protocol Engine can run on any array member. Load balancing can determine the best array member to use based on CPU load at the time. It also chooses the least-loaded application tier server from a list configured on a per-application basis. This two-phase load balancing can also take physical network locations into account, utilizing the Intelligent Array Routing feature to ensure that the appropriate servers are chosen to make best use of network and hardware resources.

With round-robin DNS or other third-party solutions you can also ensure users log in to servers evenly across the array.

Array and load balancing features together provide improved reliability and usability, and ensure business continuity:

- If one site fails, users can access applications provided by other sites instantly, with no reconfiguration.
- To handle increased load, application tier servers and Sun Secure Global Desktop Software servers can be brought into service transparently with no user disruption.
- For essential hardware or operating system maintenance, application tier servers and Sun Secure Global Desktop Software servers can be taken out of service with minimal user disruption.
- Information about users and their applications is replicated across the array, and managed from anywhere.
- Users are insulated from all details of array members and application tier servers—they just log in and access their applications.

Centralized Administration

Elizabeth Blue uses Sun Secure Global Desktop Software every day—it works just as she wants it to. So does Bill Orange, who works in Indigo Insurance’s Information Services department. But he has additional requirements and responsibilities: he needs to keep the users happy and ensure the service is always available.

The Sun Secure Global Desktop Software architecture is designed for people like Bill. He doesn’t need to visit client devices—Sun Secure Global Desktop Software client components are downloaded and configured automatically for users logging in using a Web browser. He doesn’t need to visit application tier servers—Sun Secure Global Desktop Software Protocol Engines speak the application tier servers’ language so no extra software is required. Instead Bill can manage users, applications, Webtops and the array from anywhere, using a combination of graphical and command-line tools. And to scale to more users, Bill simply adds a Sun Secure Global Desktop Software server to the array—again without touching client devices or application tier servers.

If Elizabeth wants a new application on her Webtop, Bill runs Object Manager (he can run it from anywhere—as he’s a Sun Secure Global Desktop Software administrator, it’s on his Webtop). Object Manager lets him search or browse the Sun Secure Global Desktop Software datastore, which contains objects representing people, applications and hosts, collected into organizational units. Bill can create an object to represent Elizabeth’s application (if it doesn't already exist), and drag it onto the panel that shows her current Webtop (this panel is associated with Elizabeth’s own “person” object). Using other panels he can find out which applications Elizabeth is running, and even shadow an application—allowing them both to use the application at the same time. This lets Bill troubleshoot application usage wherever he is—even while travelling, saving more time and effort. Alternatively, simple application publishing tasks can be handled through use of the Configuration Wizard, also available on the Webtops of Sun Secure Global Desktop Software administrators.

Only administrators can run Object Manager or the Configuration Wizard and define the applications that appear on people’s Webtops. With Sun Secure Global Desktop Software controlling access and all application tier servers safely out of direct contact from client devices, Bill can be sure that Elizabeth can access the applications she’s authorized to access and no others.

Should Indigo Insurance use a Directory Services database to store their user information, application provisioning can be easier yet. Once Bill has described an application—what it looks like, what applications servers can run it, load-balancing policy, and so on—he then publishes it so that users can access the application as described above. With Directory Services Integration (DSI), Bill can specify which users receive applications access based on the contents of the organization's directory service. For example, he can publish applications to users who are members of a particular group, or who belong to a certain department, or who have a specific job title. This simple, yet powerful feature reduces administration and since the associations are resolved at application launch time, there's no chance of using 'stale' data—users who are transferred from one department to another will see the new applications immediately upon login, without a single change being made in Sun Secure Global Desktop Software.

Alongside Object Manager Bill can run Array Manager. This tool gives him an overview of the whole array and the servers it contains and lets him add or remove array members. He can change array-wide settings such as the authentication mechanisms currently in use, and add new license keys when the array needs to accommodate more users. He can also change settings that apply to each array member, such as location (used for Intelligent Array Routing) and whether users are currently allowed to log in, useful when needing to take individual machines off-line for maintenance purposes.

All Object Manager and Array Manager functionality is available through UNIX command-line tools, and Bill can write simple UNIX shell scripts to batch-process configuration changes. For example, if Indigo Insurance acquires Aquamarine Assurance Bill can easily write a script to add all employees of Aquamarine Assurance to the Sun Secure Global Desktop Software array and assign them appropriate application access.

As mentioned previously, the Configuration Wizard can be used to perform many of the tasks handled in Object Manager or Array Manager. As the name implies, the Configuration Wizard takes a guided, step-by-step approach to performing common administrative tasks, such as adding and deleting users, applications, and servers from the deployment. This tool is a Web application, written utilizing the Web services API interface for Sun Secure Global Desktop Software, and is a lightweight alternative to the full administration tools. It also serves as an example application of using the API interface, so that if an organization wishes to create a custom administrative interface to Sun Secure Global Desktop Software, the Configuration Wizard code can be used as a starting point.

Accountability

Who did what, and when, are hard facts to discover in a traditional network environment. The larger the organization, the harder—but more important—they become. With Sun Secure Global Desktop Software controlling all application access, accountability and auditing become much simpler.

- Users can only access the applications available to them: if it's not on Elizabeth’s Webtop, she can't use it. Administrators control what's on everyone's Webtop.

- Application tier servers are isolated from users by Sun Secure Global Desktop Software servers. Even if Elizabeth can access an application on a server through her Webtop, she doesn't have complete access to that server. Administrators control application tier servers.
- Users can authenticate themselves to Sun Secure Global Desktop Software servers in a number of ways, including RSA SecurID two-factor authentication. This form of authentication can increase security by combining information from a hardware "token" belonging to Elizabeth with her secret PIN. Whichever authentication method is used, administrators control which users can log in even down to the IP addresses they can log in from.

Comprehensive logging tracks all application access across the array. Information about the user sessions of Elizabeth and all her colleagues, including application start and stop times and application tier server information, can be output in CSV format for processing using third-party applications.

Adaptive Internet Protocol (AIP)

In today's organizations, users need access to their applications from anywhere: from the office, where they might be hot-desking; from home, using a slow connection; or even on the move, via wireless networks. They might be using powerful desktop workstations, laptop PCs, network computers or PDAs.

The Adaptive Internet Protocol makes no assumptions about client capabilities or bandwidth: it measures and adapts, so the user doesn't have to. The goal of AIP is to deliver the best user experience it can in varying network conditions.

AIP is used between Protocol Engines running on the Sun Secure Global Desktop Software server and Display Engines running on the client device. AIP carries user input and display updates, plus print jobs and files accessed through the client drive mapping feature. It can also deliver audio traffic to a client from sound-enabled Windows applications. When used in conjunction with an optional security pack, all AIP traffic is encrypted.

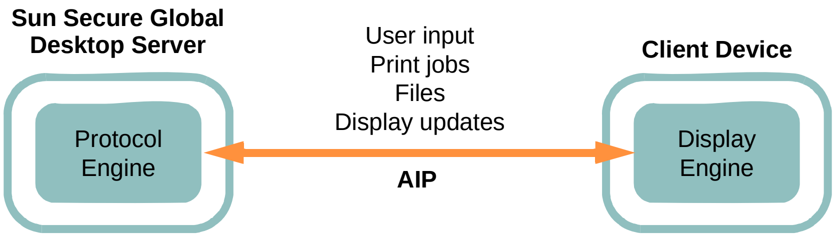


Figure 4. Adaptive Internet Protocol (AIP) Engine

Measurement and Adaptation

AIP optimizes the user experience by using heuristic mechanisms to measure the current conditions, and then by adapting the way data is transferred across the network between the user's client device and the Protocol Engine running on the Sun Secure Global Desktop Software server. If the network conditions change, so does AIP.

Feedback on client device performance, network latency and available bandwidth dictates how much processing the Protocol Engine performs, and how many operations are performed by the client device. The Protocol Engine classifies the level of optimization required and makes adjustments automatically. For example, AIP differentiates between "interactive" applications (where there's keyboard and mouse input) and "streaming" applications (where most display updates aren't a direct result of user actions) and applies a different set of optimizations to each. For an interactive application, AIP tries to ensure that user inputs are seen as quickly as possible. For a streaming application, it's important for the user to see all of the display updates (for example, all frames of an animation).

AIP measures bandwidth and latency using data transferred during normal application usage, or (if application usability won't be affected) by sending a small number of extra packets, typically every few minutes.

Fine-tuning AIP

Administrators can fine-tune AIP settings for each graphical application to ensure the best user experience. These parameters can be set:

- ***Command compression*** determines whether AIP compresses commands for transmission. With high-bandwidth connections (for example, where the client and Sun Secure Global Desktop Software server are on the same LAN), compression incurs a greater overhead than transmitting commands uncompressed. The default is Adjust Dynamically, which enables or disables compression according to the network conditions.
- ***Command execution*** determines whether AIP always executes commands in order, or optimizes commands for performance reasons. For some applications, for example those that use animation, the order in which commands are executed is critical. The default is to Adjust Dynamically based on network conditions.
- ***Interlaced images*** determines whether images are transmitted and displayed in a series of interlaced passes, or in one pass from top to bottom. Interlacing is recommended for graphics-intensive applications, particularly over low-bandwidth connections. The default is Adjust Dynamically, which enables or disables interlacing according to the network conditions.
- ***Graphics acceleration*** specifies whether acceleration is allowed. Acceleration optimizes graphics rendering and improves performance, at the expense of smoothness and exactness. For example, colors may not always be exact. If your application's display must always be exact, you should disable acceleration.
- ***Delayed updates*** specifies whether delayed updates of the display are allowed. This accumulates changes and can improve performance. If your application's display must always be exact, you should disable delayed updates. We recommend you turn off delayed updates for animation or when using Sun Ray ultra-thin clients.

SmartColor

The Adaptive Internet Protocol includes SmartColor handling for those applications that require high color depths. For UNIX applications, the following parameters can be set on a per-application basis:

- ***Color depth*** specifies the color depth of the application: 8, 16 or 24 bits. The greater the number of colors, the more memory is required on the Sun Secure Global Desktop Software server and on the client device, and the more network bandwidth is used between them. To reduce network bandwidth at greater color depths, change the Color Quality setting.
- ***Color quality*** specifies the effective color depth displayed on client devices. It reduces the number of distinctive colors in the application display before sending it over the network. Reducing color quality reduces bandwidth usage, but also reduces the number of colors displayed on the client device. The default setting fixes the color depth at the most appropriate setting according to network conditions at the time the user starts the application. Another setting allows the quality level to change at any time depending on network conditions (quality can vary from 12-bit to 24-bit color for 24-bit color applications, and from 6-bit to 16-bit color for 16-bit color applications). If necessary administrators can specify the color quality precisely, from 24-bit down to 6-bit color.

Allocating Bandwidth

In addition to the attributes for controlling AIP on a per-application basis, another attribute applies per-person:

- ***Bandwidth limit*** specifies, for each user, the maximum bandwidth that user may consume between the client device and the Sun Secure Global Desktop Software server for graphical applications. This allows administrators to provide a common level of service to all users, regardless of their connection speeds. By default, users may consume as much of the available bandwidth as possible, but administrators can restrict each user to any bandwidth in the range 10Mbps down to just 2400bps.

Administration and Management Tools

Sun Secure Global Desktop Software includes two comprehensive graphical management tools written in the Java programming language, as well as multiple command-line tools and simplified Web based tools. Only designated administrative users can run these tools, which are published on administrator Webtops for convenient access

These tools have been designed for scalability and ease of use, and allow centralized administration of arrays of Sun Secure Global Desktop Software servers from anywhere, using any client device.

Object Manager

Object Manager, which can be run from the Webtop or command line, is a scalable, search-based administration tool for managing users and applications throughout an organization. Property sheets let administrators set up a user's details, including their name and Email address, the applications they're authorized to access from their Webtop, and even how much network bandwidth they can use for AIP. Similar property sheets allow configuration of applications and application tier servers. Objects may be collected into organizational units to reflect the structure of an organization.

Using simple drag and drop actions, administrators can configure users' Webtops and set up application tier server load balancing.

With Object Manager, administrators can easily find out which users are currently running which applications, and can shadow an application session and interact with the application at the same time as the user. All actions apply to the entire array, giving administrators control over application access across the organization from a single point.

Array Manager

Array Manager is an easy to use tool for setting up and managing Sun Secure Global Desktop Software server arrays. Like Object Manager, it can be run from the Webtop or command line.

Administrators can configure array-wide settings, such as the login page that all users see, the license keys in use, and which mechanisms to use for user authentication (for example, a separate LDAP server or RSA SecurID authentication).

Administrators can also add and remove Sun Secure Global Desktop Software servers from the array, promote a secondary server to be the primary server, and configure settings for each server independently. For example, if a server needs to be "decommissioned" temporarily (for example, for an operating system upgrade) you can easily stop users logging in to their Webtop using that server.

Configuration Wizard

The Configuration Wizard is a Web-based application which provides quick access to basic administration functions, such as adding a user or publishing a new application. The interface guides the administrator through each requisite step in the process. For example, when adding an application the administrator is asked to define which application tier server(s) the application should run on, and which users should have access to it. This interface is useful for novice administrators and to provide quick access to simple functions. By necessity, it is a simplified interface, and not every option or attribute is available. Object Manager, Array Manager and the command line tools can be used for more sophisticated requirements.

Session Manager

The Session Manager is another Web application available on the administrators' Webtop, and is used to provide a quick interface for administrators to see which users are logged into the array, what applications they're running, and to view other details on these user sessions.

Command-line Tools

Using the command line tools, an administrator can perform all Object Manager and Array Manager functions (using batch scripting if desired), and more. For example, administrators can query the log files, list currently spooled print jobs, or populate the application tier server password cache.

Application Connectivity

The three-tier architecture of Sun Secure Global Desktop Software enables support for multiple application types from a single Sun Secure Global Desktop Software server or array.

Sun Secure Global Desktop Software gives users access to applications of these types:

- **Microsoft Windows applications**, running on Microsoft Windows 2000 Server or Microsoft Windows Server 2003. Sun Secure Global Desktop Software Webtops can also provide access to applications installed locally on Microsoft Windows clients, allowing administrators to present users with a single interface to all their applications.
- **Sun Solaris OS, Linux and other UNIX X Window System applications**, running on any industry-standard server. Client-side X servers are also supported (although session resumability is not possible in this case).
- **Sun Solaris OS, Linux and UNIX and Linux character applications**, running on any industry-standard UNIX or Linux server. VT420, Wyse 60 and ANSI character applications are supported.
- **Web applications** protected by Basic HTTP authentication, for example servlets.
- **Java applications**, either running using a client-side JVM (through the user's Web browser) or a server-side JVM.
- **3270 applications**, using the Sun Secure Global Desktop Software Mainframe Connectivity Pack (installed separately).
- **5250 applications**, using the Sun Secure Global Desktop Software AS/400 Connectivity Pack (installed separately).

No additional software needs to be installed on any application tier server to allow application access through Sun Secure Global Desktop Software. Applications can be deployed to users without additional application tier server resources or downtime. However, an optional enhancement module can be installed on application tier servers for additional functionality.

Connection Methods

Connections can be made to application tier servers using a number of different protocols, such as telnet or SSH. An SSH solution is not supplied as part of the product and the host operating system must supply SSH if this option is enabled in Sun Secure Global Desktop Software.

Arrays

A single Sun Secure Global Desktop Software server can handle several hundred users. Each user logs in to the Sun Secure Global Desktop Software server to see their Webtop, and the server keeps track of all application sessions while maintaining network connections to all logged-in users.

When the limits of a single Sun Secure Global Desktop Software server are reached, you can add more to create an array. With arrays of just a handful of servers you can easily handle several thousand simultaneous users.

As far as a user is concerned, all array members are equivalent. A user can log in to any array member, and they'll see the same Webtop. Array members share all application and user information, including details of running sessions. If a user starts an application while logged in to one array member, and then logs in to a different array member, they can continue using the application exactly where they left off.

Load balancing ensures that application sessions are distributed evenly across the array. See "Load balancing" in this document for more details.

Array members can be in different physical locations: in fact, anywhere with a network connection, whether LAN or WAN. For an organization with multiple distributed data centers, Sun recommends at least one array member for each data center (depending on user load).

A key goal of arrays is to ensure that access to applications is always available. Geographically dispersed arrays and data centers help to guarantee business continuity in almost all scenarios.

Array Structure and Administration

An array contains:

- One primary server. This is the authoritative source for array-wide information.
- Any number of secondary servers. Information is replicated to these servers by the primary server, using the Java Object Serialization Interface (JOSI) protocol over port 5427/TCP.

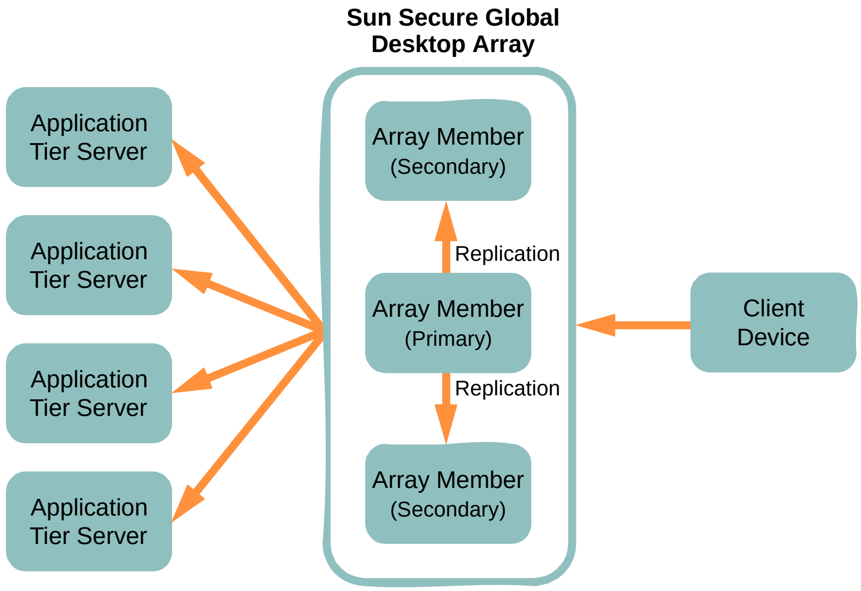


Figure 5. Sun Secure Global Desktop Software Array Structure Conceptual View

A single, "standalone" server is considered to be the primary server in an array with no secondary servers. With this approach administrators always manage the array as a single entity, no matter how many members the array contains. Like the Internet, arrays "route around" failure. If an array member is unavailable, other array members take up the slack. If the primary server is unavailable, administrators can promote a secondary server.

The administration tools Object Manager and Array Manager let you view and edit array-wide information. Object Manager administers users, applications and the organizational structure for the array. Array Manager is used to construct arrays and set both array-wide settings and settings that apply to each array member.

Server Lockout

Sun Secure Global Desktop Software allows administrators to “decommission” servers within an array for maintenance, upgrades, etc., without affecting users. This stops new users from logging in to a particular server, without affecting existing users, and redirects new users to other array members.

Example: Business Continuity

Here's an example of how arrays of Sun Secure Global Desktop Software servers ensure business continuity and guarantee application access.

Our fictional company Indigo Insurance has two offices in Boston and Seattle, each with a data center. Each office also has a Sun Secure Global Desktop Software server, and these servers are joined together as an array so that they share information about users, applications and sessions.

Elizabeth Blue is working from the Boston office, logged in to the Sun Secure Global Desktop Software server in that office. She's running an application hosted in the Seattle data center, and load balancing has ensured that the Sun Secure Global Desktop Software server in Seattle manages the application connection (which allows the Adaptive Internet Protocol to be used on the slower network between Elizabeth’s client device in Boston and the Sun Secure Global Desktop Software server in Seattle).

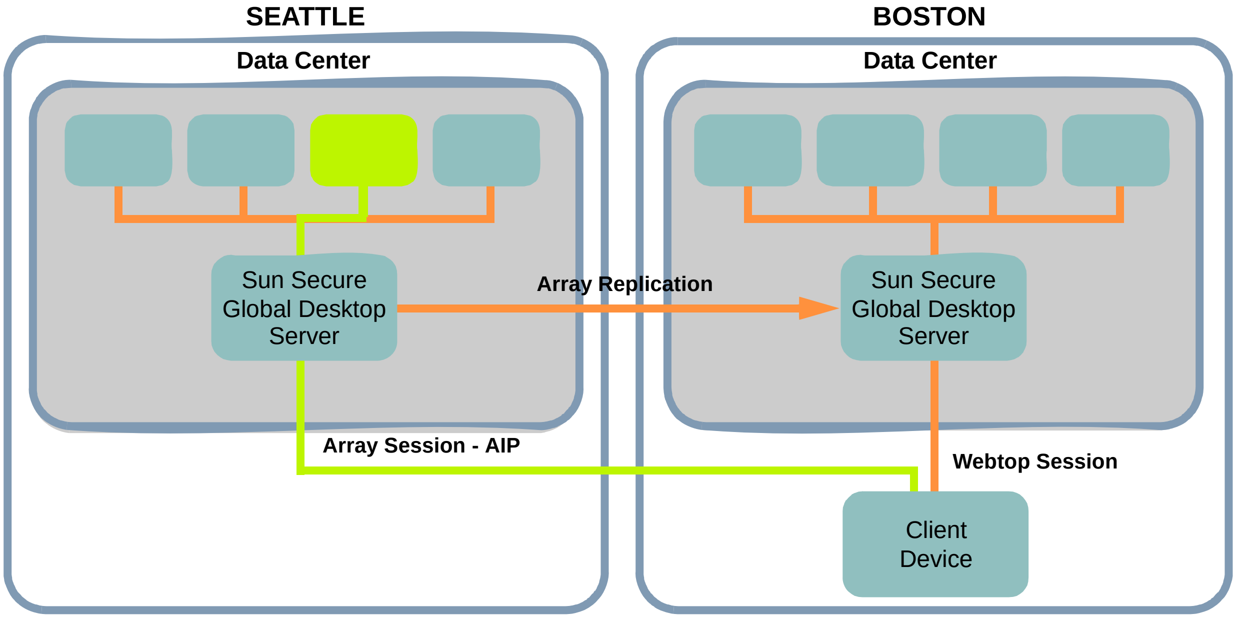


Figure 6. Webtop Session Server View: Elizabeth’s Webtop session is managed in Boston, but her application session is managed in Seattle

What happens if the Boston office suffers a power failure? Elizabeth simply dials in to the corporate network from a battery-powered laptop, and logs in to the Sun Secure Global Desktop Software server in Seattle. Her Webtop shows that she can immediately resume working with the application, exactly where she left off. The Sun Secure Global Desktop Software server and application, both running in Seattle, were unaffected by Boston's outage. And the Adaptive Internet Protocol adjusts to the reduced bandwidth, so application usability and Elizabeth's productivity aren't negatively impacted.

Authentication

With Sun Secure Global Desktop Software, users first authenticate themselves to the Sun Secure Global Desktop Software server or array to see their Webtop, and then authenticate themselves to the application tier server for each application they run from their Webtop. Administrators can allow users to save application tier server authentication details in the Sun Secure Global Desktop Software secure password cache so they're not prompted for those details again.

Sun Secure Global Desktop Software Array (Webtop) Authentication

To see their Webtop, users must first log in to the Sun Secure Global Desktop Software server or array. To allow organizations to integrate Sun Secure Global Desktop Software seamlessly with their existing IT infrastructure, users can be authenticated in many different ways by configurable login authorities. User credentials (username and password) are sent from the client device to the Sun Secure Global Desktop Software server, where each login authority in turn uses its own set of rules to map the credentials to an appropriate object in the Sun Secure Global Desktop Software datastore, and to try to authenticate the user against an authentication service. If authentication succeeds, the object located by the login authority in the Sun Secure Global Desktop Software datastore determines the content of the user's Webtop.

User credentials are encrypted between the client device and the Sun Secure Global Desktop Software server only if the Sun Secure Global Desktop Security Pack is in use (or if using Web server authentication and an appropriately configured secure HTTP server). Without the Sun Secure Global Desktop Security Pack, credentials are obfuscated but not encrypted.

Administrators have full control over which login authorities are in use across the array. For more details of the login authority mechanism see the product documentation, which is also available on the Sun Web site.

The following services can be used for authentication:

- LDAP
- Microsoft Active Directory
- Windows domains
- RSA ACE/Server (for RSA SecurID two-factor authentication)
- UNIX user database (including NIS)

Sun Secure Global Desktop Software can also be configured to detect whether users have already been authenticated by the Web server (by Basic HTTP authentication as defined in Internet RFC 2617), removing the need for additional authentication when logging in to their Webtop. This can be particularly convenient when a custom or proprietary authentication module has already been written for the Web server. In this way, Sun Secure Global Desktop Software is abstracted from the requirement to interface with an assortment of different authentication modules, and instead need only interface with one, the Web server.

Anonymous access to a Webtop can also be allowed, if desired. Users can log in without supplying a username or password and be given access to certain applications using a pre-populated password cache, where the administrator has specified a username and password to be used on the application tier server, without this information being changeable or viewable by the user.

Application Tier Server Authentication

To run an application from their Webtop, users must log in to the application tier server that hosts the application. Sun Secure Global Desktop Software presents the user with the appropriate authentication dialog for the type of application tier server, and forwards the credentials to the application tier server on behalf of the user.

The Sun Secure Global Desktop Software array maintains a secure application server password cache, which can store user credentials if the security policy of an organization permits this. If credentials are already cached for a user when they run an application, they're passed automatically to the application tier server and the user isn't prompted. Sun Secure Global Desktop Software's ability to learn and cache the credentials of users implements a form of single sign-on capability, which can greatly simplify the end-user experience, by not having users repeatedly prompted for login information. Administrators can use administration tools to add, edit and remove entries from the password cache.

Sun Secure Global Desktop Software includes support for application tier server password expiry, and where possible allows the user to change their password if the application tier server indicates it has expired.

Caching of Array Credentials

Administrators can control whether users' array credentials are also stored in the application tier server password cache. This can be useful where an array member is also an application tier server. The application tier server password cache is encrypted using triple-DES.

Sun Secure Global Desktop Software clients allow caching of array credentials on the client device (when used with a particular command-line argument). In addition, if an array is configured to detect whether users have been authenticated by a Web server, the Web browser may cache those credentials.

Client Drive Mapping

Users logging in to Sun Secure Global Desktop Software and running a remote Windows application can access their client computers' disk drives from these applications as though they were network drives. For example, users can work on documents using applications displayed through Sun Secure Global Desktop Software, and then save the results to their local client's floppy drive or hard drive.

The Adaptive Internet Protocol is used for sending all data to and from client drives. This ensures best use of the available bandwidth, and when used with the Sun Secure Global Desktop Security Pack ensures that all traffic is encrypted across the network.

Sun Secure Global Desktop Software administrators can configure which users have access to which drives, which drives to map (by drive letter, such as 'C:' drive, or by type of drive, such as 'removable'), which mode (e.g., "read-only") and which drive letters to use on the application tier server. Users who are using UNIX or Linux clients to access Windows applications use a file to specify their drive mappings, such as mapping "$HOME" on their local client to an "H:" drive on the Windows server.

The Sun Secure Global Desktop Enhancement Module must be installed on Windows 2000 / Server 2003 application tier servers to allow users to access their local drives.

Client Support

Sun Secure Global Desktop Software supports client access using three different mechanisms. There are two ways to access a Sun Secure Global Desktop Software deployment from a Web browser and a third method of access utilizing a stand-alone program installed on the client device called the Sun Secure Global Desktop Software Native Client. Each type of access is described in the following sections.

The Browser-based Client

The browser-based client supports leading Java technology-enabled Web browsers, including recent versions of Mozilla Firefox, Microsoft Internet Explorer, and Safari (for Mac OS X users), without requiring additional software to be manually installed. Sun Secure Global Desktop Software manages client software installation and version maintenance automatically.

The browser-based client is comprised of two separate parts, the helper and the client component. The helper is a Java applet that delivers and installs the client component and maintains the state of the Webtop as application sessions are created and ended (technically, the helper is optional and the browser-based client can be used without it in environments where Java is unavailable—however, in this case, functionality is reduced). In contrast, the client component is written in native code for each supported platform and handles the high performance display of applications and user interaction, as well as AIP communication with the Sun Secure Global Desktop Software server.

The browser-based client is the most full-featured way to access an Sun Secure Global Desktop Software server and is generally the recommended client when there is no compelling reason to use one of the other provided mechanisms. To use the browser-based client, users simply click the Log In link on a Sun Secure Global Desktop Software server's default index page and the client component will be started, with an automated installation step inserted if necessary.

The Java Client

The Java client is referred to in Sun Secure Global Desktop Software as the “classic” client because it was the standard client used in versions of Sun Secure Global Desktop Software prior to 4.0. The Java client provides excellent cross-platform portability and simplifies setup when firewalls are used, but has limited Webtop functionality when compared to the browser-based client. Similar to the helper module in the browser-based client, the Java client is an applet that is automatically run when a user clicks the “Log In (classic Webtop)” link on an Sun Secure Global Desktop Software server default index page.

Native Clients

Standalone applications known as Sun Secure Global Desktop Software Native Clients are available for some client platforms and devices. The native client does not require a Java Virtual Machine or even a Web browser and is useful in environments that are incapable of running these additional products due to limited memory, storage or other resource issues. The native clients offer similar functionality to the Java client with none of the advanced features of the browser-based client.

Administrators can give native client users access to a Web browser on an application tier server through their Webtop. This allows centralized control, through the application tier server hosting the Web browser, of browser versions and access policies.

Users can download Sun Secure Global Desktop native clients directly from the default index page of a Sun Secure Global Desktop Software server or download them from the Sun Download Center.

Load Balancing

Sun Secure Global Desktop Software performs three types of load balancing:

- Emulator Session load balancing, which determines the Sun Secure Global Desktop Software array member that runs the Protocol Engine for the application session.
- Application tier server load balancing, which determines the application tier server that executes the application.
- Intelligent Array Routing, which is used in conjunction with the other two methods to ensure that connections between Sun Secure Global Desktop Software servers and application tier servers use high-speed links.

In addition, as users may log in to any array member to see their Webtops, it's possible to balance users' Webtop sessions across array members using standard techniques such as round-robin DNS and load-balancing switches, among other techniques. This fourth type of load balancing is not included with Sun Secure Global Desktop Software.

Emulator Session Load Balancing

When users start an application, a Protocol Engine is started on one of the Sun Secure Global Desktop Software array members to act as a proxy connection to the application running on an application tier server. Protocol engines communicate using a specific protocol type, such as X11 (for X-Windows), the Remote Desktop Protocol (RDP) for Windows applications, and so on. An instance of a Protocol Engine is called an emulator session. When a user launches an application, the required emulator session can be started on any Sun Secure Global Desktop Software array member and the decision as to where to start the emulator session is handled by the Sun Secure Global Desktop Software emulator load balancing algorithms. The administrator may define the load-balancing policy for the array; based on CPU usage (load is continuously measured across the array) or number of sessions (the number of application sessions being managed on each array member). The default setting is to start the emulator session on the array member the user is currently logged into (where their "Webtop" session is connected).

Application Tier Server Load Balancing

Application tier server load-balancing is the ability of Sun Secure Global Desktop Software to select an application tier server to run an application based on pre-defined selection criteria, generally, the server with the most available resources at the point in time of the launch request. For an application to be load-balanced in this way, the administrator defines an application, and then defines the application tier servers that can run that application. The administrator then defines the load-balancing policy for that application, if different from the array's default policy. The policies include "Most Available CPU Resources", "Most Available Free RAM", or "Fewest Application Sessions."

Sun Secure Global Desktop Software determines the resources available on each application server by use of the installation of an Enhancement Module for that particular application server type. These Enhancement Modules determine the capacities and current load of each server, and report this data to the Sun Secure Global Desktop Software Array. This information is updated regularly, and distributed throughout the array. Should an application server stop reporting, is marked as "down", and no further application sessions will be requested on that server until it resumes normal operation.

The parameters which control the behavior of the enhancement module data collection and reporting mechanisms are tunable by the administrator, so that, for example, a more frequent sampling frequency can be defined.

Intelligent Array Routing

Intelligent array routing works with array load balancing and application tier server load balancing to try to make best use of network resources. Where possible, array members and application tier servers are chosen with the same location (as configured by administrators)—even if this means choosing an array member or application tier server with a greater load. This ensures that the native, bandwidth-intensive protocol (e.g., X11 and RDP) used between the Sun Secure Global Desktop Software array member and the application tier server uses the fastest network connection, allowing the Adaptive Internet Protocol, which optimizes bandwidth usage, to travel the potentially much greater low-bandwidth distance between the client device and the array member.

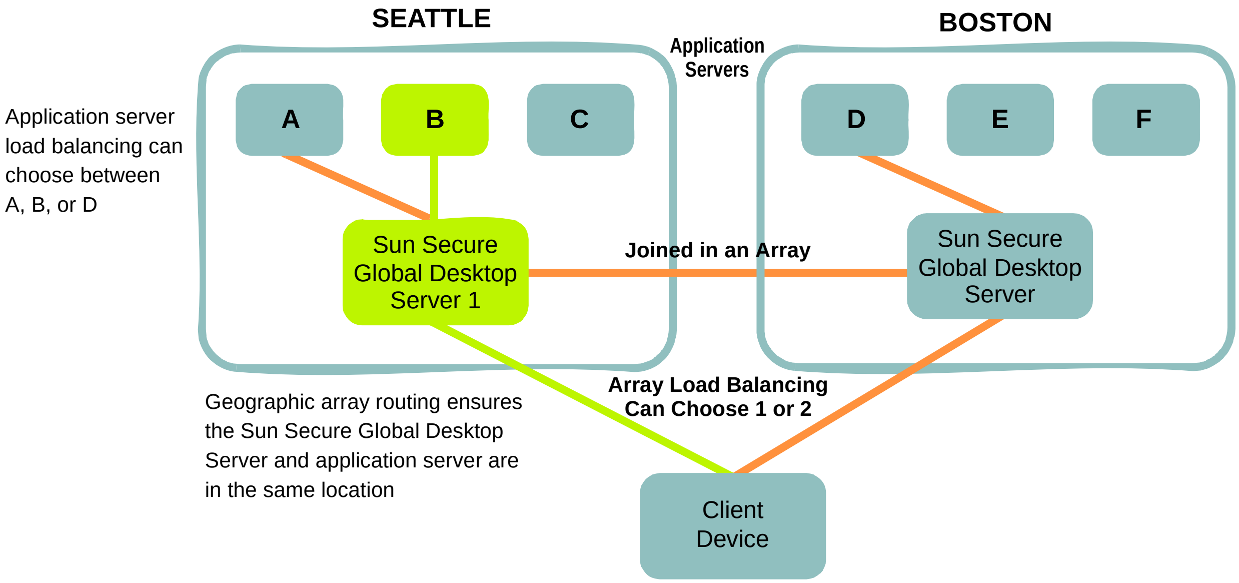

SEATTLE
BOSTON
Application Servers
Application server load balancing can choose between A, B, or D
A
B
C
D
E
F
Sun Secure Global Desktop Server 1
Joined in an Array
Sun Secure Global Desktop Server
Geographic array routing ensures the Sun Secure Global Desktop Server and application server are in the same location
Array Load Balancing Can Choose 1 or 2
Client Device

Figure 7. Intelligent Array Routing

The diagram gives an example of how intelligent array routing, array load balancing and application tier server load balancing work together. In the diagram, two data centers and a client device are illustrated. Data center 1 is in Seattle and contains one Sun Secure Global Desktop Software server and three application tier servers (A, B, and C). The second data center is in Boston and has a similar configuration (the application tier servers in Boston are labelled D, E, and F). The Sun Secure Global Desktop Software servers in each location are joined together in an array. Application Tier Servers A, B, and D are all of the same type and have the same applications installed. A user requests an application hosted on these application tier servers. As was discussed earlier, to fulfil the request an emulator session must be instantiated on a Sun Secure Global Desktop Software server and the application must be run on an application tier server.

To comply with the intelligent array routing parameters as defined by the administrator, there are only three acceptable combinations of Sun Secure Global Desktop Software servers and application tier servers:

- Sun Secure Global Desktop Software server 1 with application tier server A
- Sun Secure Global Desktop Software server 1 with application tier server B
- Sun Secure Global Desktop Software server 2 with application tier server D

In this example, Sun Secure Global Desktop Software server 1 and application tier server B are chosen, as they are the least loaded combination of the three possibilities.

Printing

In the same way that Sun Secure Global Desktop Software allows users to access their applications securely from any client device, users can also print securely from those applications to local printers attached to their client devices. Users login from many different locations and they expect printed documents to be routed to and formatted properly for the printer attached to the system they are using. Sun Secure Global Desktop software can do exactly this.

When a user prints from an application displayed through Sun Secure Global Desktop Software, a print job is created on the application tier server using an appropriate printer driver on that server. The print job is passed to the Sun Secure Global Desktop Software server through either an RDP interface (for Microsoft Windows 2000/ 2003 applications) or an LPD interface (for UNIX/Linux applications.).

The Sun Secure Global Desktop Software server includes a print subsystem that receives print jobs from the application tier servers and spools them for delivery. Specialized print Protocol Engines are used to translate (if necessary) and transfer print jobs to the client device using AIP (if the user has a secure connection, this traffic will be encrypted). The print Display Engine then sends the print job to the designated printer on the client device.

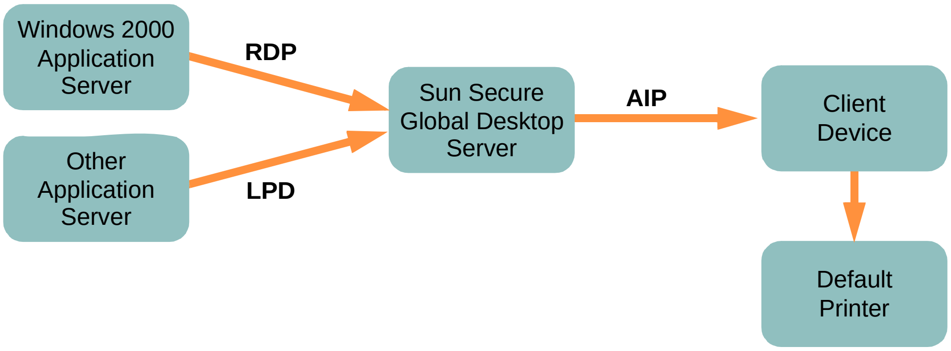

Windows 2000 Application Server
Other Application Server
RDP
LPD
Sun Secure Global Desktop Server
AIP
Client Device
Default Printer

Figure 8. Printing System — How print jobs are transferred from the application server to the client's default printer.

Users can pause and resume printing as well as cancel print jobs using controls on their Webtop. If a user's client device does not have a configured printer, print jobs remain spooled on the Sun Secure Global Desktop Software server. The next time the user logs in from a client with a properly configured printer they can resume printing.

Windows RDP Printing

With Microsoft Windows 2000 and Server 2003 application tier servers using Windows Terminal Services, client device printers are automatically detected and equivalent printer(s) configured on the application tier servers, each with the appropriate printer driver. These printers are actually pseudo-printers which forward print jobs to the Sun Secure Global Desktop Software server's print queue, which then transfers the print jobs to the client printer(s) using a "print" channel in the AIP protocol. The process of auto-creating Windows printers is called "RDP Printing", and is very convenient and transparent to both the administrator and the user.

Because of printer model naming differences, the automatic detection of printers on the client device only works with Windows-based clients. For other client types, the mapping of printer models to local print queues is done via a client-based configuration file, wherein printers will still be automatically created for the user, using a specified driver type, and the automatically created printer will be associated with a local client print queue.

While RDP printing provides users a transparent, secure, and high-fidelity printing mechanism, there is one requirement of RDP printing which can prove problematic in certain environments. For RDP printing to work properly, the application tier server must recognize the client printer type and the client printer drivers must be available on the application tier server. If the printer driver is unavailable on the application tier server, then Windows has no way of determining the proper printer language to use for the pseudo-printer and RDP printing fails to work properly.

In environments where the set of printers is well-known and controlled, this limitation can be overcome by ensuring that the proper printer drivers are installed on the application tier servers. However, in more general purpose environments this can be extremely problematic. For example, if a Service Provider is providing application services to the general public there is no way to make certain that every potential printer driver is installed on the application tier servers. Fortunately, Sun Secure Global Desktop Software has an alternative for this scenario called “PDF Printing.”

PDF Printing

A flexible alternative to the RDP / LPD based print system, PDF Printing leverages the high quality Adobe Portable Document Format to provide reliable, consistent, cross platform printing for clients that have the free Adobe Acrobat Reader installed on their systems.

PDF Printing is quite simple. When a user logs into a Windows application tier server, a virtual printer is created utilizing a high quality, high-fidelity printer driver known to be available on the server. By default, this virtual printer is pre-configured as an HP Model 8500 PostScript Color Laser printer, but this option can easily be modified by the administrator. When a user prints to this virtual printer a PostScript file is created (PostScript is a high quality, platform-neutral printer language) and is sent to the Sun Secure Global Desktop Software server where this file is rendered into a PDF document. This PDF document is then sent to the client device and opened in Acrobat Reader where it can be printed using the client's normal printing mechanism. Optionally, the file can be sent to the client device without being printed, which provides a handy way to create PDF documents.

Security

Sun Secure Global Desktop Software includes a number of security features built into the base distribution, but several additional features are available in the Sun Secure Global Desktop Security Pack. These advanced features require additional configuration and are not part of the base install for this reason. Installing the Security Pack enables the use of these features.

In the following list of highlights, features marked with (*) require the Sun Secure Global Desktop Security Pack to be installed and configured.

- Support for HTTPS Web servers (note that this does not secure Adaptive Internet Protocol traffic—for that you need the Sun Secure Global Desktop Security Pack).
- The ability for administrators to set access policies based on client device (defining secure connections requires the Sun Secure Global Desktop Security Pack).
- Support for SSH connections between Sun Secure Global Desktop Servers and application tier servers.
- Isolation of application tier servers in the data center from users and potential attackers (this feature is called "Protocol Isolation").
- The ability for administrators to have full control over the applications each user is allowed to access.
- Full auditing of application access across the array.
- Support for firewalls, including DMZ environments.
- Support for RSA SecurID two-factor authentication (*).
- Support for SSLv3 / TLS 1.0-secured encrypted connections between client devices and Sun Secure Global Desktop Software servers with support for the Advanced Encryption Standard (AES) 128 & 256, as well as 3DES and RC4 encryption ciphers (*).
- Sun Secure Global Desktop Software server identity validation using X.509 server certificates (*).
- Support for test certificates and supplementary certificate authorities (*).
- Support for client-side proxy servers, including authenticating proxies (*).
- Support for single-port firewall traversal (*).

Configurable Access Policies

Administrators can configure whether each user has a secure or standard connection, or is denied access, based on the client device and Sun Secure Global Desktop Software server they're using. For example, a user can be given a secure connection whenever they connect from a client device outside the firewall, and a standard connection when connecting from inside the firewall.

To configure secure connections requires the Sun Secure Global Desktop Security Pack.

Firewalls and Proxy Servers

When the Sun Secure Global Desktop Security Pack is installed, Sun Secure Global Desktop Software enables application access by supporting authenticating proxy servers (for Web browser users and Sun Secure Global Desktop Native Client users) and by providing firewall traversal functionality in which all network traffic to and from the Sun Secure Global Desktop Software server passes over a single port, usually 443/TCP (the standard HTTPS port).

This is critical when there are intervening firewalls between the client system and the Sun Secure Global Desktop Software server because it's very difficult to “open” ports in firewalls due to security policies, especially when the firewall configuration is managed by another organization. TCP port 443 is a well-known port, and is generally an allowable opening in most firewall configurations. This lets you support these scenarios:

- Where client devices are on sites not managed by the organization that controls the Sun Secure Global Desktop Software servers, or where such connections pass though other organizational domains.
- Where client devices are configured to use proxy servers, which may require additional authentication.
- Where network traffic is routed through firewalls: between the client devices and the Internet, and between the Internet and the data center hosting the Sun Secure Global Desktop Software servers and application tier servers. Security policies at each firewall restrict which ports are opened to the Internet.

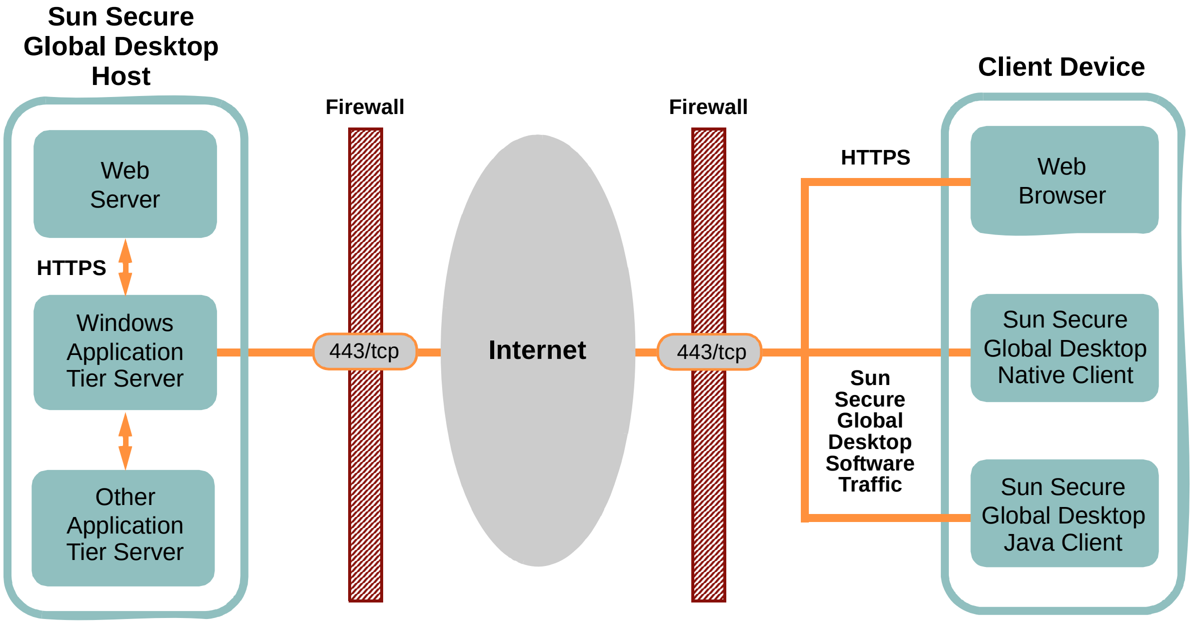

Sun Secure Global Desktop Host
Web Server
HTTPS
Windows Application Tier Server
Other Application Tier Server
Firewall
443/tcp
Internet
Firewall
443/tcp
HTTPS
Sun Secure Global Desktop Software Traffic
Client Device
Web Browser
Sun Secure Global Desktop Native Client
Sun Secure Global Desktop Java Client

Figure 9. Security — Accessing Sun Secure Global Desktop Software through firewalls

Recommendations

- Use a secure (HTTPS) Web server on all Sun Secure Global Desktop Software hosts. This ensures that all Web pages users see, and the sensitive connection information the Secure Global Desktop client component downloads, are encrypted. Using a secure Web server does not encrypt application session information, such as key presses, display updates or login information, so you must install the Sun Secure Global Desktop Security Pack for this level of security. A combination of the Sun Secure Global Desktop Security Pack and HTTPS is recommended.
- Use test certificates only for testing purposes. For a production array, we recommend you use X.509 certificates obtained from recognized Certificate Authorities.
- Configure firewalls to allow only essential network traffic, and access control lists to control source and destination addresses. For details on how to configure firewalls for use with Sun Secure Global Desktop Software, see the Sun Secure Global Desktop Administration Guide (available on the Sun Web site).

Please note that the security features of Sun Secure Global Desktop Software and the Sun Secure Global Desktop Security Pack are intended to be used in conjunction with, and not as a replacement for, standard security practices.

Session Management

All information regarding user application sessions is stored on a Sun Secure Global Desktop Software server in the array. The centralized session management approach allows users to move from client device to client device without disrupting their running applications. It also allows “help-desk” activities, where users can temporarily allow their application session to be shared with an administrator.

Session Resumability

Session resumability lets users resume an interrupted session, on any client device, at a later time. For example, Bill Orange, currently running an application at the office through Sun Secure Global Desktop Software, turns off his PC and goes home. When Bill arrives home, he can log back in to Sun Secure Global Desktop Software from any supported client device and resume the application, as if he was still at his desk in the office. While Bill travels home, the application continues running. He could start a lengthy calculation in the office, and then pick up the results when he logs in from home.

Session resumability is also useful for applications that take a long time to start, or for those that require the user to take a large number of steps after start-up (for example, to walk through a complicated menu system).

Session resumability also allows for interrupted network connections. For example, if a user is connected via modem and the line drops, then session resumability ensures that applications aren’t disrupted and dialing in again will allow the user to continue where they left off.

Administrators can configure session resumability per-application. There are three options:

Webtop session resumable: The application continues to run until the user explicitly logs out of their Webtop. This ensures that transient problems such as network outages or browser instability don’t affect application usage. The user can just log in again and resume work.

Always resumable: The application continues to run, even if the user logs out of their Webtop. The user can log in and log out as often as they like, without affecting the application.

Never resumable: The application exits as soon as it disappears from the Webtop. Selecting a never-resumable application on a Webtop always starts a new instance of the application.

Resumable applications continue to use system resources while the user is logged out. To help control resource usage, administrators can configure a timeout value for each application: a timer starts when the user disconnects or (for always resumable applications) logs out, and the application will be terminated once the timeout is reached.

Shadowing

Session shadowing allows administrators to view and interact with a user's Sun Secure Global Desktop Software application sessions simultaneously with the user, so that both keyboards and pointing devices are simultaneously active. Help-desk staff can take over a user's application session and get them out of trouble or otherwise assist.

When an administrator tries to shadow a session users are always prompted and can accept or decline.

The Sun Secure Global Desktop Software server can log session shadowing activity, including shadowing requests, whether the request is accepted or declined, when the shadowed session is suspended or ended, and when the shadowing ends.

There is another type of shadowing supported, called “Classroom Shadowing”, in which a single user (or “instructor”) can host and interact with an application, while multiple viewers (“students”) can connect to and view the running application, typically in “view-only” mode. Classroom shadowing is useful for providing training or similar guided demonstrations to multiple viewers simultaneously.

Webtop

Users interact with applications and documents on the network using the Web equivalent of a desktop—the Webtop. Sun Secure Global Desktop Software gathers all applications and documents associated with a user—the Webtop content—and dynamically creates a page to represent this information.

Users can start any application Web-enabled by Sun Secure Global Desktop Software simply by clicking the application's link on their Webtop. Applications can be displayed within the browser, as a separate integrated window, or even full-screen without any window decoration. A Webtop can include applications installed on the client, for example a Windows front-end to a client/server application, allowing a common access method for all applications wherever they're hosted.

Each user can be configured with personal Webtop content that no other user sees. In addition, Webtop content can be assigned based on position within the organization. For example, a financial application can appear on the Webtops of everyone in the Finance department. And applications can be placed on the Webtop of every user in the organization, with one drag and drop action.

Webtop Customization

The browser-based client Webtop is pure HTML, dynamically generated by a Web application written in Java Server Pages (JSP) and utilizing the Web services APIs in Sun Secure Global Desktop Software. The source code for the Webtop application is included on the Sun Secure Global Desktop Software server and can easily be customized by administrators with the appropriate skills.

The Webtop application communicates with the Sun Secure Global Desktop Software server using standard Web service methods like SOAP and XML. This means that the entire Webtop application can be replaced with a portal, for example, or a custom Webtop application written in any number of languages on any standard platform.

Note that the Sun Secure Global Desktop Native Clients do not use HTML or Java and are not customizable.

Glossary

This section describes in more detail the architectural components not fully defined elsewhere.

Datastore

The Sun Secure Global Desktop datastore is the sum of all the information used by the various components of Sun Secure Global Desktop Software. The datastore includes:

- Information about hosts and users on the network
- Sun Secure Global Desktop Software session information (users logged in, applications running)
- Organizational information

This information can be manipulated with Object Manager, Array Manager or from the command line, and is accessible array-wide.

To ensure that all objects in the datastore can be addressed, Sun Secure Global Desktop Software uses a naming scheme known as Tarantella Federated Naming, or TFN. TFN, Based on X/Open Federated Naming, TFN ensures that information from multiple differing sources can be identified in a well-defined way.

Each object in the datastore has a unique TFN name. TFN names include a component identifying the source of the information, called the namespace. TFN names commonly have the following form:

```
.../namespace/name-within-namespace
```

The “...” indicates the "root" of TFN. Each namespace may use a different naming scheme. The namespace part of the TFN name acts as a "gateway" to that naming scheme. The following namespaces are commonly used with Sun Secure Global Desktop Software:

Namespace	Example	Description
ENS	.../_ens/o=Indigo Insurance/ou=Marketing/cn=Cust-o-Dat	Objects with Secure Global Desktop-specific behavior
LDAP	.../_ldap/cn=Cust-o-Dat,ou=Marketing,o=Indigo Insurance	Objects in an LDAP server
DNS	.../_dns/verona.indigo-insurance.com	Hosts on the network

Table 1. Sun Secure Global Desktop Namespaces

Display Engine

Display Engines are part of the Secure Global Desktop Client component, running on the client device.

Each running Display Engine has an Adaptive Internet Protocol connection to a Protocol Engine running on a Sun Secure Global Desktop Software server. A Display Engine sends mouse and keyboard input to the Protocol Engine, and receives and renders application display updates from the Protocol Engine.

A Display Engine starts when a user clicks an application on their Webtop. This causes the Protocol Engine Manager to start an appropriate Protocol Engine if necessary, and connect the Display Engine and Protocol Engine together. They then communicate directly (and securely via the SSL Daemon, if the Sun Secure Global Desktop Security Pack is in use and the user is configured for a secure connection), independently of other parts of the Sun Secure Global Desktop Software server.

Sun Secure Global Desktop Software uses one Display Engine per application for each user. For example, a Character Display Engine starts when a character application is requested.

JServer

The JServer runs on the Sun Secure Global Desktop Server. It is the decision-making process that maintains configuration information and the object database.

The JServer handles application launch and resumption, load balancing, session management, array replication and authentication. It connects to the Protocol Engine Manager to launch applications and verify UNIX passwords. It is event-based and propagates important events across the array. JServers on different array members communicate on port 5427/TCP.

The JServer is written in the Java language. The JServer appears in process listings as “jre”, as it is hosted by a Java Runtime Environment process.

Protocol Engine

Protocol Engines run on the Sun Secure Global Desktop Server. They provide the emulation necessary to view and interact with an application, and act as a client to the application on the application tier server—communicating using the application tier server's native protocol, such as X11 or RDP. A Protocol Engine translates this native protocol into Adaptive Internet Protocol (AIP) for transmission to the Display Engine on the client device. Protocol Engines are implemented as native binaries to ensure optimal performance on the server.

Graphical applications such as X11, Microsoft Windows, 3270 graphical and 5250 use the Graphics Protocol Engine. Character applications use the Character Protocol Engine. Other Protocol Engines are the Print Protocol Engine and the Client Drive Mapping Protocol Engine.

Sun Secure Global Desktop Software uses one Protocol Engine for each application type for each user. However, each Protocol Engine process can handle multiple application sessions for a particular user. Protocol Engines are invoked on demand.

Protocol Engine Manager

The Protocol Engine Manager hands off Adaptive Internet Protocol connections to Protocol Engines and executes application tier server logins. It communicates with the JServer on a dynamically allocated port to:

- Access the application tier server password cache
- Receive application server login requests
- Notify the JServer when emulator sessions change state

The Protocol Engine Manager appears in process listings as “ttaauxserv”.

SSL Daemon

The SSL Daemon handles secure connections between client devices and the Sun Secure Global Desktop Server. It encrypts and decrypts network traffic and forwards it to the appropriate components. It communicates with the client component on port 5307/TCP and with the JServer on port 5427/TCP.

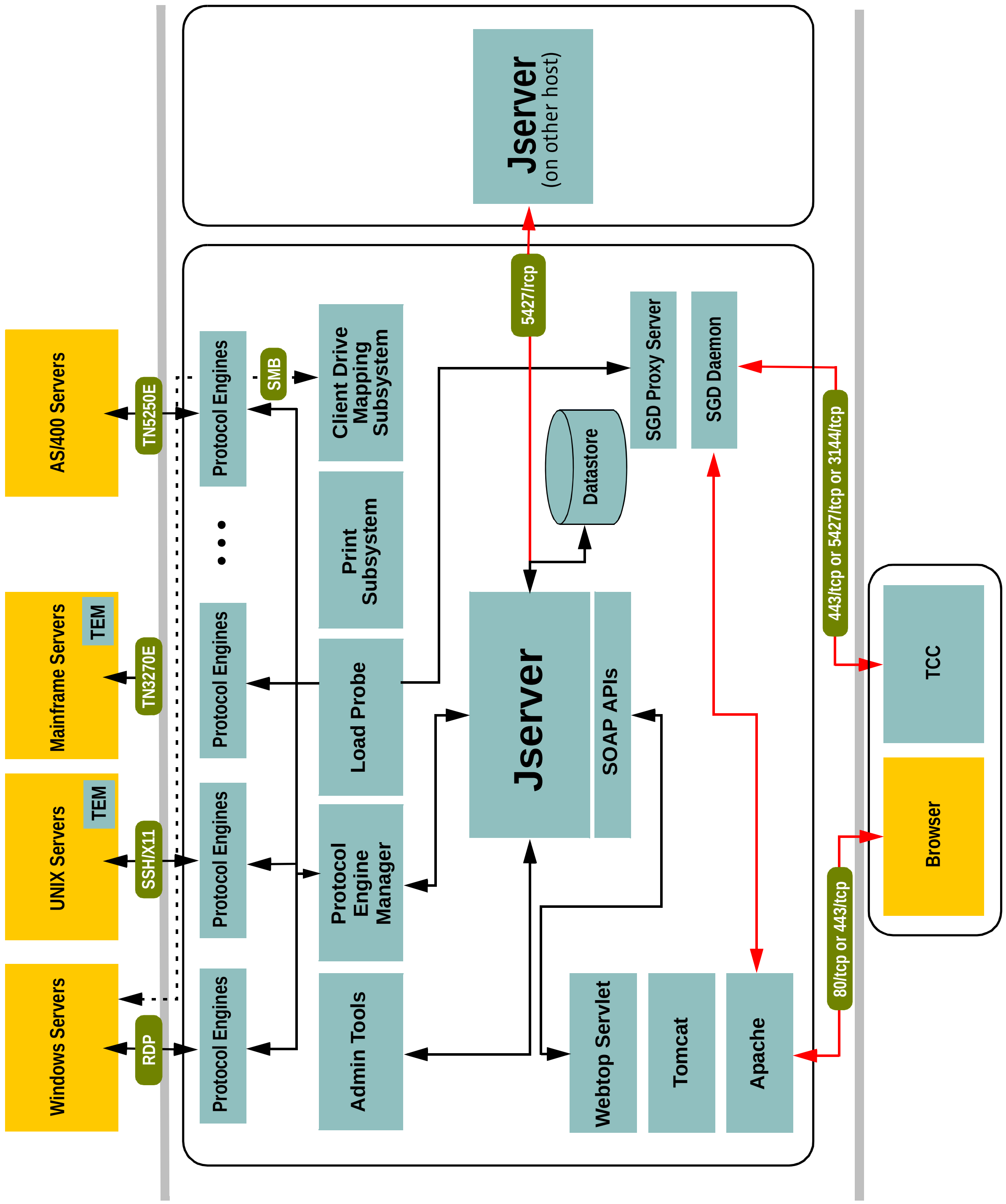
The SSL Daemon appears in process listings as “ttassld”.

Sun Secure Global Desktop Proxy Server

The Sun Secure Global Desktop Proxy Server is the controlling parent process of the Sun Secure Global Desktop Software server, and starts the Protocol Engine Manager and JServer. It sends launch requests to the Protocol Engine Manager and passes all other requests to the JServer. It communicates with the client component on port 3144/TCP and with the JServer on port 5427/TCP. It will restart the JServer and Protocol Engine Manager if they exit unexpectedly.

The Sun Secure Global Desktop Proxy Server appears in process listings as “ttaauxserv” (the same as the Protocol Engine Manager, as the parent Proxy Server process forks to assume two roles).

Sun Secure Global Desktop Software Architecture Diagram



Supported Servers, Client Devices, and Web Browsers

Refer to www.sun.com for updated information.

Sun Secure Global Desktop Software Installs on these UNIX or Linux Servers	• Solaris 8, 9, and 10 OS (SPARC® Platform Edition) • Solaris 10 OS (x86 Platform Edition)	• SUSE LINUX Enterprise Server 8, 9 (x86) • Red Hat Enterprise Linux 3, 4 (x86) • Fedora Core 3, 4 (x86)
Provides Access to These Application Types	• Microsoft Windows • Solaris (character and graphical) • Linux and other UNIX (character and graphical)	• Mainframe (3270) • AS/400 (5250) • HTML • Java
Using These Protocols	• Microsoft RDP • X11 • HTTP, HTTPS	• Character (ASCII and ANSI) • TN3270E • TN5250
Sun Secure Global Desktop Software Server Requirements	• 200MB free disk space, plus another 100MB at install time • Minimum 512MB RAM	
Sun Secure Global Desktop Software Server Requirements Per User (Note that screen resolution and color depth will affect memory requirements)	• 5MB RAM for each user • 10MHz to 15MHz for each user • Additional 12MB per user for each X application • Additional 12MB per user for each Windows session • Additional 0.9MB per user for character applications • Additional 1.5MB per user for each 3270 or 5250 application	
Supported Client Devices	• Leading Java technology-enabled clients, including Microsoft Windows, Sun Java™ Desktop System, Linux, and Mac OS X: • Windows XP Professional: Internet Explorer 6.0+, Netscape™ 6.0+ • Windows 2000 Professional: Internet Explorer 6.0+, Netscape 6.0+, Mozilla Firefox 1.4+ • Solaris 8+ SPARC: Netscape 6.0+, Mozilla/Firefox 1.4+ • Solaris 10 x86: Netscape 6.0+, Mozilla/Firefox 1.4+ • Red Hat Enterprise Linux v3.0 Desktop: Netscape 6.0+, Mozilla/Firefox 1.4+ • SUSE Linux 9.1 Personal Desktop: Netscape 6.0+, Mozilla/Firefox 1.4+ • Mac OS X 10.2+: Safari 1.2.3 • Sun Secure Global Desktop Native Client-enabled devices including thin clients, wireless PDAs, and Pocket PCs	
Network Transport	TCP/IP	

Table 2. Supported Servers, Client Devices, and Web Browsers

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com