

Frequently Asked Questions about

VIVIDESK Systems

Centre for Health Evidence



VIVIDESK Systems FAQ

Introduction	4
What is VIVIDESK?	4
What does VIVIDESK do?	5
What features are commonly used?	5
What benefits result from desktop management?	6
Top 3 reasons to use VIVIDESK	7
About this Manual	7
Architecture	8
What is the architecture of a VIVIDESK solution?.....	8
What functions do VIVIDESK components perform?	8
Infostructure	10
What computer hardware is required?	10
What are the minimum hardware requirements for the VIVIDESK client?.....	10
What are the minimum hardware requirements for the VIVIDESK server?.....	10
What operating system is required?.....	12
What operating systems are supported?	12
Are different versions of VIVIDESK required for different versions of Windows?	13
Can Macintosh computers view VIVIDESK desktops?.....	13
What database management system is required?.....	13
What database products are supported?	13
What degree of data segregation is supported?	13
What application software is supported?.....	14
What Software types are supported?	14
What Internet technologies are supported?	15
Can VIVIDESK be launched from a web page link?.....	15
What software incompatibilities are known?	15
What user privileges are required?	16
What workstation user privileges are needed to install VIVIDESK client software?.....	16
Security	17
Security Model	17
What types of security needs are addressed by VIVIDESK?.....	17
How does VIVIDESK support and enhance security?.....	17
How does VIVIDESK manage security?	18
How are users authenticated?	19
What authentication types are supported?.....	19
Can users be authenticated from an LDAP or Active Directory?	20
Can strong authentication be enforced?	20
Can more than one user be logged on at the same time?.....	21
How easy is it to change users?.....	21
Where are authentication credentials stored?	21
How are users authorized?.....	22

What categories of authorization are supported?	22
Can security be set at the individual user level?.....	23
Can the system assign users to roles or groups, and assign security at that level?....	23
Can administrative roles be delegated to different groups?	23
Can users change their passwords?	24
Can users be reminded about forgotten passwords?.....	24
Is there complete independence between user and workstation?	24
How are communications protected?.....	25
How are messages encrypted?.....	25
How are passwords protected on VIVIDESK servers?.....	26
How are passwords protected on VIVIDESK clients?.....	26
Does VIVIDESK support RSA, Entrust and other security products?	26
What firewall ports are required for encrypted communications?	27
Can records of conventional Internet communications be cleared?	27
How is security verified?.....	28
How is authentication integrity verified?	28
Can time-outs be set to prevent non-authenticated viewing?	28
How is non-repudiation enforced?	28
What non-repudiation methods are used?	28
What audit trails are available?	29
Can the audit capabilities be configured for different types of users and applications?29	
Can the audit capabilities be configured to exempt some items from audit?	29
Security Threats	30
How does VIVIDESK address Internet security threats?.....	30

Single Sign On 32

Can multiple applications be controlled through a Single Sign On (SSO)?	32
How does VIVIDESK SSO work?.....	32
What SSO methods are supported?	33
Can the choice of SSO method be context-sensitive?	34
Which hardware and software platforms support SSO functions?	34
Can VIVIDESK automatically close applications that it has opened?	34
Are SSO capabilities limited by firewall, dial-up or web-access constraints?	35
To what level can an administrator script into an application?	35

Remote Windows Applications 36

Application Service Provider Technologies	36
Overview	36
Citrix Metaframe	36
Microsoft Remote Desktop Protocol	37
VIVIDESK.....	37
Can VIVIDESK be used as a thin-Client for Citrix and Microsoft Servers?	37
How do Citrix, RDP and VIVIDESK technologies differ?.....	38
How do Citrix, RDP and VIVIDESK server management methods differ?	43
How do Citrix, RDP and VIVIDESK handle licensing and user fees?.....	43
What does VIVIDESK add to remote desktop services?	44
Can VIVIDESK be run on a remote desktop server?	44

Context Management 45

Does VIVIDESK support context management?	45
What context management method is used?.....	45

Usage Monitoring	46
How is data collected and what is captured?	46
What types of usage data are tracked?.....	46
In what format is VIVIDESK usage data recorded?	47
Can audit results be displayed online?.....	47
Communications	48
Can global messages be sent out?.....	48
What is the best way to add messages and applications?	48
Support	49
What is the level of fault tolerance?	49
What level of support comes with VIVIDESK?.....	50
Pilot Projects, Custom Solutions	50
Implementation.....	50
Regional Roll Out.....	50

Introduction

What is VIVIDESK?

VIVIDESK is an Internet desktop-management technology that facilitates integration of multiple information sources, networks and technologies in a simple, customized, centrally managed information environment.

- VIVIDESK provides secure single sign-on access to Internet, network and local computer resources and technologies.
- VIVIDESK facilitates standards-based application-to-application messaging, allowing multiple information resources to share a common decision-making context.
- VIVIDESK is a pioneer in delivering services through the use of a Distributed Desktop Technology.

VIVIDESK:

- presents a clean, simple interface
- combines information resources to reflect each user's interests and experience
- supports group-specific tips, announcements, and communications tools
- administers electronic surveys and interactive exercises, and immediately compiles results
- monitors use of each application and captures data about how users interact with the computer system
- handles multiple authentication methods for commercial software and licensed resources
- simplifies access to information
- delivers information in multimedia formats

At either voluntary or time-out sign-off, VIVIDESK systematically logs off and closes all software and resets the interface, ready for the next log-on.

What does VIVIDESK do?

The "VIVIDESK Desktop" refers to the VIVIDESK technology and the functionality that comes with the VIVIDESK Client-Server application. The VIVIDESK Desktop technology delivers and manages customized Internet "Desktops" which provide simplified access to a wide range of information resources.

VIVIDESK provides **users** with:

- a simple, secure, customizable, user-friendly computer interface for personal computers;
- a well-established robust product;
- tried and tested and operates on all Microsoft operating systems and can be simulated in a Macintosh environment;
- highly flexible and tailorable to the needs of specific virtual communities.

VIVIDESK allows **organizations** to provide health professionals with:

- secure, private, authenticated online information environments;
- integrated access to knowledge, learning, and practice resources;
- custom resource packages for different disciplines, specialties, interests;
- interactive collaboration, communication, and education tools;
- access to multiple licensed resources via a single sign-on;
- network wide announcements, alerts and guidelines.

VIVIDESK allows **administrators** to:

- create site-specific collections of commercial, institutional, and Internet-based software, appropriate for each type and level of user;
- control access to confidential data, but avoid multiple logon passwords;
- automatically distribute software or software updates to users with no intervention;
- monitor system performance and usage through automated data collection and graphical data displays;
- administer electronic questionnaires at first log-on and at predefined intervals if requested.

What features are commonly used?

VIVIDESK can be customized based on the needs of your organization.

Key features that are commonly used include:

User management – project administrators can organize users into different groups, manage accounts; includes online registration system.

Application management – project administrators can customize desktop content and assign resources to different groups.

Interests management – project administrators can code desktop content using keywords, users can then customize their own content display.

Single sign-on – users can store their account information for member only sites in the system.

Multilanguage – if budgeted, organizations can build a VIVIDESK desktop in the language of their choice.

Monitoring – project administrators can view usage statistics, including number of logons, time logged on and number of minutes that each application resource was used.

My Workspace – users can store and manage their own personal contacts, bookmarks, documents, and notes.

My Settings - users can manage their own contact information, email settings, and account information.

Help System – built in VIVIDESK Help manuals and tutorials for users and administrators.

Web Browsing – built in web browser for searching the Internet and storing bookmarks/favorites while minimizing exposure to malware.

Communications – configurable mail system allows users to access, send, and delete mail messages stored on home or office email system (based on IMAP service); includes built in quick mail where appropriate.

Survey management – project administrators can build custom questionnaires; includes variety of question types, branching, anonymity, and the ability for users to pause a survey and return later to complete it.

File management – designated users can manage group document collections; includes ability to add, edit, delete multiple file types (Word, PDF, PPT, MHT, HTM).

Bulletin Board – allows designated desktop users to post messages to the bulletin board; includes start/end date feature so that messages area is automatically populated/archived.

Please note that VIVIDESK includes additional capabilities not listed – if you have a complex information management need, contact us to find out if VIVIDESK will work for you (info@vividesk.com).

What benefits result from desktop management?

VIVIDESK offers benefits for all stakeholders, including end users, administrators and their organizations as a whole.

USER	BENEFIT
Individual	<ul style="list-style-type: none"> ○ Simple and easy to use. ○ Access to a customized set of applications and resources.

USER	BENEFIT
	<ul style="list-style-type: none"> ○ Single interface for multiple resources. ○ Only one password required. ○ Accessible from any PC with an Internet connection.
Administrator	<ul style="list-style-type: none"> ○ Simplifies user account management. ○ Resources are easily added or removed. ○ Resource usage is tracked and audited. ○ Central management and distribution via group profiles.
Organization	<ul style="list-style-type: none"> ○ Customization allows for integrity of corporate branding and image. ○ Reduced administration time and costs. ○ Improved flow of information. ○ Increased productivity. ○ Greater security. ○ Reduces server bottlenecks. ○ Minimal server infrastructure needs.

Top 3 reasons to use VIVIDESK

1. VIVIDESK is a vendor neutral approach to the centralized management of remote desktops in complex enterprises.
2. VIVIDESK is a managed desktop solution that offers cost-effective integration of all knowledge and clinical applications.
3. VIVIDESK supports quality improvement and research with detailed usage monitoring.

About this Manual

This "frequently asked questions" manual is intended to address information needs of system administrators seeking technical details about the security and integration capabilities available to VIVIDESK systems. This manual assumes comfort with computer and networking terminology. Please note that VIVIDESK installations will vary depending on organizational preferences. Although there are a number of standardized VIVIDESK configurations, the system also serves as an advanced integration toolkit. Modular in design, a wide range of custom functions can be activated, developed or adapted to meet the needs of complex organizations.

Architecture

What is the architecture of a VIVIDESK solution?

VIVIDESK is a client-server solution that follows a three-tier design model. Its architecture consists of well-defined and separate processes, each executable on a different platform:

1. **Client:** the user interface which runs on the user's computer
2. **Server:** the functional modules that actually process data, running on an application server and accessed over the Internet
3. **Database management system (DBMS):** a compatible data processing system that stores the data required by the middle tier and runs on a database server

Although a VIVIDESK solution always consists of client, server and database components, it is possible to install all three on the same computer device, as may be done when running a VIVIDESK stand-alone 'kiosk' or for testing purposes.

Most VIVIDESK solutions include knowledge and document management components. These require a fourth layer, provided by a compatible Internet Information Server.

What functions do VIVIDESK components perform?

A "Desktop" refers to the selection and organization of information resources that are presented and supported for a particular user group. The visible pages, application icons, visual interface, and availability of electronic mail, discussion groups, diary and inventory functions are all desktop-dependent.

Presentation of unique, centrally managed, desktops for multiple users is accomplished with VIVIDESK's client-server architecture, built with modern Internet component technology.

A small VIVIDESK **client** component executes on the user's computer. This establishes a secure connection with its server using proprietary HTTP requests on port 8080. The client forwards the user's request for access to a particular VIVIDESK Desktop.

The VIVIDESK **server** responds with information about required logon and authentication methods and sets up a secret key encrypted communication channel. If authentication expectations are met, then the server provides the client with all instructions needed to build a user-specific single-sign-on desktop. The 'zero footprint' client stores all desktop-configuration information -- including protocols for accessing multiple applications -- encrypted in volatile memory, with nothing appearing in registries, temporary disk files,



cookies, or other formats. Once instructed by the server, no further client-server communications are needed until log-off, when the client returns usage and audit information to the server. Between log-on and log-off, the client 'checks-in' with the server at pre-determined intervals to validate its security key, upon which many functions depend.

The VIVIDESK server, in turn, communicates with one of the supported **database management system(s)** where desktop, user, group, interest, authentication and usage data is securely stored.

Infostructure

What computer hardware is required?

What are the minimum hardware requirements for the VIVIDESK client?

The VIVIDESK system is an Internet technology that uses a thin Internet client to manage private communications with Internet server computer(s). The client component is installed from the Internet and is then available for making connections to any number of Web servers, other Internet servers, local software on the computer workstation and one or more VIVIDESK servers.

Essentially, if a computer can run Internet Explorer 4.0 or more recent, then it will be able to run VIVIDESK. This usually translates into the following minimum hardware requirements:

- 500 MHz central processor, or better
- 256MB memory
- Windows 98, Windows 2000, Windows XP, Windows 2003, or Windows NT (version 3.51 and higher)
- 3 MB of hard drive space
- Internet Explorer 4.0 or higher (it is recommended that Internet Explorer 5.0+ be installed with 128 bit encryption compatibility)
- An Internet connection (48 kilo baud or faster modem; fast Internet connection using DSL, Cable or better recommended)

What are the minimum hardware requirements for the VIVIDESK server?

VIVIDESK server functions can all be performed on a single Internet server computer configured with Microsoft Internet Information Server, version 3.0 or more recent. It is also possible to distribute VIVIDESK server functions over multiple server computers, and so balance server loads for high-volume VIVIDESK implementations.

The following VIVIDESK server functions can reside on one server or on multiple linked server computers:

- **REQUIRED:**
Primary VIVIDESK server. (user authentication, security, single-sign-on capabilities)
Multiple primary servers can be set up to serve different VIVIDESK desktops or all desktops can be served from the same primary server. VIVIDESK server technology also works with load-balancing server clusters.
Because VIVIDESK is a single-sign-on manager, the computer running a VIVIDESK server must have a valid certificate for secure socket layer (SSL, https) communications.
- **OPTIONAL:**
Secondary (backup) VIVIDESK server.
A VIVIDESK client switches over to this server if it cannot connect to its primary server in a timely fashion. The same computer can serve as both primary and secondary VIVIDESK server.
Primary and secondary servers can use the same data and communications stores.
Because VIVIDESK is a single-sign-on manager, the computer running a VIVIDESK server must have a valid certificate for secure socket layer (SSL, https) communications.
- **OPTIONAL:**
Installation and update server.
A distinct machine can be designated to manage client installations, automated updates, and version monitoring. This is important because high-volume VIVIDESK environments can trigger levels of file uploads and downloads can be disk-intensive .
- **OPTIONAL:**
World-Wide-Web server.
Desktops may link to a variety of conventional Web pages (html, xml, aspx, etc.) which can be stored on the same server as the VIVIDESK server or, in high use situations, on one or more separate servers.
- **OPTIONAL:**
Electronic Mail server.
Desktops can integrate electronic mail communications and discussion lists with other information services. A VIVIDESK email server can be used and installed on a the same server as the VIVIDESK server software. A separate machine can also be used and other email software can be substituted for the VIVIDESK email service.
- **OPTIONAL:**
Data server.
A VIVIDESK server can be configured to use Microsoft Access 2000 or Access XP databases. This is most economical. A VIVIDESK server can also be configured to use most SQL database products. The primary and secondary VIVIDESK servers can share the same data server and the data server can be installed on the same machine as the VIVIDESK server. In general, projects expecting up to 200 simultaneous logins (usually this corresponds to 20,000 or more users) will perform well with a combined VIVIDESK/data server using an Access database. Busier projects will notice performance improvements with an SQL database engine.
- **OPTIONAL:**
Remote Desktop Protocol or Citrix Metaframe server.
VIVIDESK supports Microsoft's remote desktop protocol (RDP) for running Windows applications over the Internet. The Microsoft Advanced Terminal Server client is built-in to VIVIDESK. The Citrix ICA client is also supported. Because terminal server activities can tax the processing and storage resources of a server, it is possible to designate one or more separate servers for supporting RDP applications if these will be used by a project.
- **OPTIONAL:**
Internet Conference server.

VIVIDESK can be configured in "virtual community" modes to include integrated support for Internet conferencing where users are able to chat, share files, work on a joint white-board and share desktop applications with other users at different locations. The VIVIDESK conferencing client works on Microsoft Internet Information servers, with VIVIDESK taking care of user authentication, conference scheduling and other administrative functions. If this feature is to be commonly used within desktops, then it is best to designate a separate communications server (possibly shared with a web or media server).

- **OPTIONAL:**

- **Streaming Media server.**

- VIVIDESK can be configured in "virtual classroom" and "learning community" modes both of which make extensive use of streaming video and media services for demonstration and teaching purposes. Because these services can place a heavy load on an Internet server, it is best to dedicate a machine as a media server when usage exceeds 5 simultaneous video downloads.

Technical requirements for the VIVIDESK server(s) are determined by the network size, anticipated number of simultaneous users, and anticipated interval between archiving of VIVIDESK usage data.

For a low volume VIVIDESK server setup, with up to 100 simultaneous logins at any instant, a single server (Pentium 200MHz or better, 128MB RAM, 4GB hard drive) running Internet Information Server version 3.0 or Personal Web Server version 3.0, using Microsoft Access 2000 databases, is adequate. Note that the VIVIDESK Internet communications are highly efficient. Very large numbers of users can be logged on and using VIVIDESK at the same time. Hardware limitations tend to occur at the exact moment of user logon. 100 simultaneous logins could occur in projects with 20,000 or more users of which 1000 or more might be using the desktop at any one time.

For a medium volume VIVIDESK server setup, with up to 250 simultaneous logins occurring at any instant, a single server (Dual processor Pentium V 1GHz or better with high-performance hard drive) running Internet Information Server version 5.0 or better, using Microsoft SQL Server databases, should be more than adequate. An active project with 50,000 or more users could be served with such hardware.

For higher-volume configurations, it is suggested that the project needs be discussed with VIVIDESK technical experts. Depending upon particular requirements for web, conferencing, media and other Internet services, it is likely that multiple servers with differentiated functions will be recommended. It is likely that both primary and secondary VIVIDESK servers, or a load-balanced server cluster, will optimize performance when used in conjunction with a dedicated SQL database server.

What operating system is required?

What operating systems are supported?

VIVIDESK helps information system administrators and users get the most out of Microsoft Windows computers. To use VIVIDESK 's interface management and data collection capabilities, the VIVIDESK thin-client should be installed on Windows 98, Windows ME, Windows NT (3.51, 4, 5), Windows Me, Windows 2000, Windows XP, Windows 2003 or Windows VISTA computers. VIVIDESK is also available in a format optimized for Microsoft Terminal Server computers, allowing it to be delivered to Macintosh and other client computers using the Microsoft Remote Desktop Protocol.

The single best test of whether a client computer will be able to use the VIVIDESK Internet plug-in, is whether that same computer can successfully run Microsoft Internet Explorer version 4.0 or more recent.

An optional separate VIVIDESK database server can be on any operating system compatible with a Windows network.

Are different versions of VIVIDESK required for different versions of Windows?

One VIVIDESK client works on all active release 32-bit Windows operating systems.

VIVIDESK is programmed using the Microsoft Visual C++/C# internet development platform using a .Net internet component architecture. All functions required to run the VIVIDESK client are embedded in the VIVIDESK code. Using "static binding", all Microsoft Windows dependencies are also embedded in the VIVIDESK code. This spares VIVIDESK from vulnerability to changes in the Windows operating system. In addition, VIVIDESK is a registered Microsoft developer, committed to ensuring VIVIDESK compatibility with any new or upcoming changes to the operating system.

Can Macintosh computers view VIVIDESK desktops?

VIVIDESK Desktops can be accessed with a Macintosh Computer by one of two methods:

1. With Macintosh OS version IX, VIVIDESK is easiest to use with Windows emulation software. It has been tested with different emulators and works with response times that are as good as Internet Explorer.
2. With Macintosh OS X or later, then VIVIDESK is best viewed using Remote Desktop Connection software for Macintosh computer. VIVIDESK servers have support for this protocol and initiate a desktop session that works exactly as it would on a Windows computer.

What database management system is required?

What database products are supported?

The VIVIDESK server uses a multi-threaded database interface optimized for high-performance data transfer.

VIVIDESK servers can be configured to use Microsoft Access 2000, XP, 2003 databases. Alternately, the server can be set to communicate with SQL databases. Microsoft SQL Server is recommended (version 2000 through 2005). Indeed, one server can use different database products (and multiple SQL products) to store information for different VIVIDESK desktops. This hybrid design allows organizations to start small, with the free Access interface, and then migrate to independently licensed SQL products as user demand merits. The migration can be incremental, moving the high-volume desktops first while keeping some prototype desktops in Access format for ease of testing.

What degree of data segregation is supported?

The VIVIDESK database architecture is designed to address healthcare privacy considerations. Each server can manage multiple "desktops". Desktop databases are segregated, allowing data/network administrators to ensure, for example, no physical connection between a database supporting one institution's desktop and another's. The following classes of data are segregated for each desktop allowing, for example, quality improvement staff to review information usage patterns without having access to any information about user identity or sign-on particulars:

- User, desktop configuration, messaging, application data
- Knowledge, document and expertise management data

- Survey, consent, feedback data
- Usage and audit trail data
- Error, performance and threat detection logs

What application software is supported?

What Software types are supported?

The VIVIDESK client software is designed as a software 'container' within which multiple optional 'viewers' can be configured. VIVIDESK has the default capability of loading, displaying and managing Windows, Internet, Remote Desktop, Citrix ICA client, VT100 and VT200 software types. VIVIDESK supports any Internet software (local or networked) that will run in Internet Explorer version 4 or later. This includes ActiveX, Java, XML and Javascript applications. In addition, custom software viewers can be added to meet unique information delivery needs (e.g., IBM 3270 terminal emulation).

The following software types are accessible through any VIVIDESK client:

- **Local Windows Applications**
Any software application that can be executed on the client Windows operating system workstation, can be initiated, controlled, scripted, and monitored by VIVIDESK. This includes legacy DOS applications (run through the Windows command console), 16-bit Windows 3.1 applications, 32-bit Windows applications and any other software adapter that is installed on the local computer workstation (e.g., custom terminal emulators). VIVIDESK can send keystrokes and mouse events to any application it initiates, even though that application is running on the local computer. It can also monitor keystrokes and mouse events for auditing purposes.
- **Remote Windows Applications**
The VIVIDESK client can start, automatically sign on to, script and monitor Windows applications run remotely over the Internet using Microsoft's Remote Desktop Protocol. It can also initiate and manage Windows applications remotely using the Citrix ICA client technology. When Windows programs are run remotely, they actually execute on a Microsoft Terminal Server computer and there is no need for any software components to exist on the client computer.
- **Terminal Applications**
An SSO-capable, scriptable, and auditable VT100/VT220 emulator can use Telnet, FTP and other protocols to communicate with legacy mainframe computer applications. The VIVIDESK terminal emulator supports macro buttons and other customizations that simplify use of older information systems.
- **Internet Applications**
VIVIDESK has a built-in Internet browser that allows Internet-based applications to be displayed and managed as an integral part of the user interface. Internet features, such as file transfer rights, can differ for different user groups. Special display options are available to simplify Internet access with, for example, rapid access to the user's most recently visited sites. The VIVIDESK Internet settings are not affected by local workstation Internet Explorer or Netscape settings and so are present for the user no matter what computer is used to access the user's VIVIDESK desktop.
- **Internet Sessions**
VIVIDESK has a special "Session" mode for Internet applications. This allows many to be open at the same time, on the same plane of the graphical interface. VIVIDESK can then facilitate communication among these multiple Internet sessions.

- **Custom Viewers**

Optional terminal emulator modules can be integrated with the VIVIDESK interface so that users interact with mainframe applications without leaving VIVIDESK. The custom software viewer appears as another "tab" on the VIVIDESK interface.

What Internet technologies are supported?

Many advanced websites make use of Internet plug-in products to facilitate the display of information, images and sound. If an Internet site requires such a plug-in and it is available or installable on the user's computer, then VIVIDESK will work with and use that technology. For example, Adobe Acrobat documents, Microsoft Office internet-format files, Shockwave videos, Streaming audio and video all work seamlessly within VIVIDESK.

Administrators can configure VIVIDESK to work with any special actions that might be triggered by right-mouse-click or other Windows events. The desktop can also be configured to specially handle usage monitoring for Internet technologies launched by the desktop.

VIVIDESK can additionally observe and communicate with any internet or windows application that is CCOW (Clinical Context Object Working group) compliant, managing information flow between such applications.

Can VIVIDESK be launched from a web page link?

Yes, the VIVIDESK client can be launched and auto-updated from a webpage.

What software incompatibilities are known?

A few specific software products could cause potential problems with VIVIDESK, depending upon how those products are configured and installed. VIVIDESK uses the http and https protocols for client-server communication using network port 80 (8080). This is how the product ensures both simplicity of maintenance and compatibility with a wide variety of network and firewall configurations. However, if another software product interrupts and possibly changes the content of http data streams through port 80, then VIVIDESK could be affected.

Examples include:

- **Virus checking software**

where web monitoring is enabled (the program may run in memory and continually check all Internet traffic for signs of viruses). This may affect the VIVIDESK automatic update program but has not been known to affect actual VIVIDESK client-server communications. Virus checking products can be configured to ignore communications going to or from a particular (VIVIDESK) server, thus bypassing any problems that may yet be discovered with network virus programs.

- **Net surveillance**

and policing programs can be set to screen for and disable URLs with certain words in them. These are blunt instruments. If "sex" is disallowed, for example, a call to "http://sexsmith.com" becomes "http://smith.com" and the link fails. VIVIDESK cannot anticipate all the letter combinations that a net policing program might prohibit. It is possible that a combination matching some letters in the VIVIDESK server address would scramble communications between the VIVIDESK client and its server. To date, this phenomena has only been observed for web pages that are viewed within VIVIDESK desktops.

- **Net optimization**

programs sometimes monitor http traffic in order to intercept certain programs and cache them or otherwise redirect them. Proxy servers often do this. This does not affect VIVIDESK but may cause

VIVIDESK 's various viewers to fail if they are expecting to handle, for example, Adobe Acrobat files and these are somehow redirected or disallowed.

What user privileges are required?

What workstation user privileges are needed to install VIVIDESK client software?

The VIVIDESK client installation program uses its own installation and update technology. First time VIVIDESK installations are accomplished with web-based, VIVIDESK-install, or InstallShield-mediated MSI-compatible installation packages.

If a Windows client computer is opened with a user profile that prohibits any software installations or any desktop alterations, then the initial VIVIDESK installation program may not complete. In this case, the installation should be performed with a user profile that has installation rights. Thereafter, VIVIDESK has permission to update its own components as demanded by its server.

VIVIDESK client installation and maintenance is easy to automate with Microsoft SMS or other remote software installation network utilities.

VIVIDESK does not write files to reserved Windows directories, the system directory or any local area network location. It does not require Windows registry access in order to install. For these reasons, it has been found to install seamlessly under most user profiles and requires an administrator to install only on the most restricted network environments.

Security

Security Model

What types of security needs are addressed by VIVIDESK?

The Internet has emerged as a powerful aid to health information dissemination. At the same time, the Internet has exposed health data to diverse security risks.

Integrated health information environments can coordinate delivery of all the information that health care decision-makers need. Trusted environments also coordinate privacy protection for multiple information resources.

The VIVIDESK collection of integration tools include security features uniquely suited to the protection of sensitive information from multiple sources delivered via diverse technologies. Examples of VIVIDESK security capabilities include:

- **Secure Single Sign On**
- **Strong Authentication**
- **Authentication Vault**
- **Secure Context Management**
- **Cookie-free Zero-footprint Information Sessions**
- **High-fidelity Audit Trails**
- **Location-sensitive Security Levels**

This section describes commonly used VIVIDESK security features. Functions that use the VIVIDESK component architecture to address specialized needs are described elsewhere.

How does VIVIDESK support and enhance security?

Although the VIVIDESK system does not, by itself, store or transfer sensitive information, VIVIDESK Desktops can include links to confidential information resources. If VIVIDESK facilitates access to such resources in a single-sign-on environment, then it is possible for sensitive information to pass between the VIVIDESK client and its server over a local area network, an Intranet or the Internet (TCP/IP). Accordingly,

VIVIDESK has been carefully designed to meet the privacy, confidentiality and security concerns of complex organizations.

If privacy is about an individual's right to control access to information about himself or herself, and confidentiality is about the responsibility of others to protect privacy rights, then security is about the methods by which privacy is declared and confidentiality is enforced.

There are five categories of VIVIDESK security functions:

- **Authentication**
is the ability to reliably identify the source of information, the recipient of information, and any agents that may have viewed or changed the information in transit from source to recipient.
- **Authorization**
is the ability to grant different persons or groups different rights to find, view, change or delete information.
- **Encryption**
is the ability to prevent recognition and interpretation of information while in transit from source to recipient and back again.
- **Integrity**
is the ability to warrant that information has not been changed or damaged in transit from source to destination and back again.
- **Non-repudiation**
is the ability to record all changes to information so that its prior state can be known and individual changes cannot be revoked without generating a traceable audit trail.

The VIVIDESK system has special features to enable security in each of the above domains. These supplement security methods embedded in most private information resources. VIVIDESK offers extra security at little or no additional administrative burden.

How does VIVIDESK manage security?

Many Internet applications, including all web (http, https, xml, xmls, etc.) pages, rely on security provisions provided by the Internet browser with which content is viewed. These applications depend upon security capabilities, and vulnerabilities, of the Windows Internet browser. Similarly, VIVIDESK can display web pages using Windows Internet browser components.

In addition, VIVIDESK establishes protected and encrypted communication channels between its client and server. These add layers of security capabilities over and above those built-in to Windows Internet communications, without Windows dependencies. In this way, VIVIDESK technology can guarantee that certain sensitive communications never appear on disk, in web logs, web page caches or communication streams likely to be monitored by spy-ware and other malicious software. VIVIDESK can also deploy extra layers of encryption not available to Internet browsers alone.

How are users authenticated?

What authentication types are supported?

The rules that govern access to VIVIDESK desktops can be configured by VIVIDESK server administrators. Although it is possible to create "kiosk" desktops that open to a custom display without user identification, most VIVIDESK configurations use either VIVIDESK internal user authentication functions or external, third-party, authentication tools. Once an authentication method has been set by system administrators, it cannot be altered by users.

- **Non-authenticated Desktops**
(Optional) Administrators (not users) can configure one or more desktop accounts in "kiosk" mode. When a user activates VIVIDESK with one of these accounts, the desktop will open to display applications and messages without asking for a user identifier and password. Non-authenticated desktops are appropriate for public-access information. They do not allow email communications, desktop personalization or diary functions. Kiosk desktops do not support management of personal identifiers and passwords for other applications (Single Sign On, SSO, or Context Management, CCOW). NOTE: kiosk mode can only be activated by authorized central administrators: there is no way for a client workstation to function this way without the specific profile and permissions being set centrally.
- **VIVIDESK Authentication**
The most common way to use VIVIDESK is to require that users be correctly identified before access is provided to a specific desktop with its information resources, communications and software applications. Upon activating VIVIDESK, the client establishes a secure connection with its server, first sending a request to the server to join a particular project or desktop. The client software obtains the user's logon identifier and password and sends these to the server. If the user is authenticated, then a VIVIDESK session is initiated. If not, logon is denied and there is no way to view the desired desktop.
- **Windows Authentication**
It is also possible to integrate VIVIDESK with the Microsoft Windows workstation logon, and Microsoft Active Directory. If so configured, then VIVIDESK uses the user name and identity as authenticated by Windows and does not post a separate userid/password request. This approach works best in environments where users must log on and off of Windows before accessing a workstation. This method also works in a Windows XP environment where multiple users can have virtual sessions open on the same machine, switching focus between them.
- **Windows Shell Replacement**
VIVIDESK can be configured such that users boot directly into a desktop, rather than the conventional Windows shell. If VIVIDESK is used instead of Microsoft Explorer or File Manager as the Windows shell, then different Microsoft Windows profiles can be associated with different VIVIDESK desktop profiles. In this case, logging on to the Windows operating system takes the user directly to the appropriate VIVIDESK desktop. Similarly, when VIVIDESK is run in an application server environment, or via a virtual private network, network sessions can be set to launch specific VIVIDESK desktops upon satisfactory logon to the secured computing environment. The combination of VIVIDESK user management with Windows profiles can greatly simplify the work of network administrators.
- **Third-party Authentication**
Other authentication protocols, programs and user registries can be linked to the VIVIDESK system. Each software product behaves a bit differently, particularly if biometric user identification is used. In general, once the user is correctly identified, then VIVIDESK is opened to a specific

user or group desktop. VIVIDESK Global has experience fashioning connections to different types of authentication registries and can create VIVIDESK components for validating users against non-VIVIDESK databases, including LDAP directories.

Can users be authenticated from an LDAP or Active Directory?

VIVIDESK can be configured to use an independent database where user names, passwords and credentials are stored. The requirement to use an LDAP or Microsoft Active Directory can be set at the user group or desktop level. When set to Active Directory, for example, the VIVIDESK logon module queries the designated Active Directory and only opens a desktop if the user is authenticated.

There are a number of options that can be set:

- **Client-side**
When set to client-side Active Directory authentication, the VIVIDESK client uses the Windows authentication source for the current computer workstation. If userid and password are accepted, then VIVIDESK launches the user profile associated with the accepted userid. This method is appropriate where desktop access is restricted to a virtual location (including Virtual Private Network) defined by a local Active Directory pointer.
- **Server-side**
The preferred method for authenticating against an Active Directory has the VIVIDESK server perform the authentication, using the network authority in force at the server network location. This has the advantage of being workstation-independent and is easier to maintain.
- **Primary Identity**
Multiple user "roles" can be supported where one primary VIVIDESK account is used for authentication and single-sign-on purposes. This capability can allow VIVIDESK users to have different working contexts that are permitted through a single Active Directory authentication profile.

Can strong authentication be enforced?

VIVIDESK administrators can set different levels of strong authentication VIVIDESK desktops. The following password management rules can be enforced, in part or in whole, for all users of a desktop. The rules can also be enforced for logon identifiers and passwords that may be used by applications that authenticate via VIVIDESK.

- **Force Password Change**
Administrators can force password changes for individuals, user groups, or entire Desktop populations, whenever and as often as needed.
- **Password Longevity**
Administrators can optionally set an interval after which a user must change a password in order to maintain personal desktop access. The interval starts from the date of first sign-on or last password change.
- **Password Length**
An optional password length can be enforced. This can, for example, force all passwords to be 10 characters or longer.
- **Case Sensitivity**
If this rule is enforced, then passwords must be entered in the correct case in order to be accepted.

- **Alphanumeric Content**
If activated, this rule forces passwords to include both letters and a specified number of numerals in order to be accepted.
- **Special Characters**
If activated, this rule forces passwords to include a specified number of non-letter, non-number, special characters.

Can more than one user be logged on at the same time?

Only one user can be logged on to a VIVIDESK desktop on a single computer at the same time. In order to protect security of information that may be contained in applications running on VIVIDESK desktops, no two desktops can be active at the same time within a single authenticated Windows session. The VIVIDESK software explicitly prohibits this and will not allow a second instance of the software to load.

That said, in a Windows XP environment, multiple users can have virtual instances of the Windows operating system on the same machine and users can switch between instances. To do so, they must pass Windows authentication protocols. VIVIDESK can be running in each virtual instance of Windows and so, technically, multiple cases of VIVIDESK are running on the same machine. Similarly, Windows Terminal Servers may host multiple client sessions, each with an instance of VIVIDESK running. In all these situations, VIVIDESK is running in a separate memory space on a Windows computer and the integrity of its information applications is maintained.

One user may be permitted to login to VIVIDESK (using the same account) on multiple machines simultaneously. This is configured through VIVIDESK Administrator and can be set to a specific number of allowed simultaneous sessions; or to just one session.

How easy is it to change users?

Desktop logon and logoff take less than 5 seconds, allowing a quick switch from one user identity to another.

A "sleep" mode is supported that allows one user to save the "state" of a VIVIDESK desktop when logging off. When that same user logs in again, at the same computer or elsewhere, the desktop is restored with exactly the same applications open to the same location as when the user logged off. This state recall includes the decision-making context and context management (CCOW) contents.

Where are authentication credentials stored?

The user names, passwords and application parameters that VIVIDESK uses to coordinate the Single-Sign-On (SSO) integration of multiple protected information resources, are stored server-side in a credentials "vault".

An alternative approach used by many SSO managers is a client-side credentials "wallet". The client's wallet contains one or more authentication clusters and is usually stored in an encrypted format on the client's local computer. The wallet approach can result in multiple instances of authentication portfolios appearing on multiple computers and is prone to tampering.

The VIVIDESK "vault" approach includes the following attributes:

- **Centralized Credential Management**
Authentication credentials never appear on a client computer, in any format. Instead, credentials are stored on a central server computer in a username/password protected SQL database. This approach is appropriate for enforced protection of sensitive public data. Security personnel can manage and revoke privileges at any time, at an application, individual, group or desktop level.

- **Protected Storage**
The authentication database can be held in a fastidiously protected network environment, behind strong firewalls, with private network protocols.
- **Encrypted Storage**
Over and above authentication database encryption, VIVIDESK executes a further proprietary encryption protocol to store credentials "double-encrypted" so that, even the highest level database administrators cannot discern the content of credential fields in the database.
- **Single-Source Credentials**
There is but one valid source for SSO credentials, with no allowance or possibility for substitution from another source.
- **Zero Footprint**
The VIVIDESK client obtains authentication credentials from its server, holds them in memory in encrypted format, and maintains no copies, even temporary ones, of any information on the user's (client) computer. VIVIDESK does not use either session or permanent "cookies", temporary internet files, cached web pages, or any other form of local credential storage.
- **Custom Communication Channel**
The VIVIDESK client and server use a proprietary communication from client to server and back. This method does not use Internet browser http requests, ports, or protocols. Accordingly, VIVIDESK communications are not available to the browser or to any of the many web-monitoring tools that could potentially observe and record SSO exchanges.
- **Masked Communication**
VIVIDESK converts all client-server communications to a custom digital format, using a multiple digits to encode each character. This digital package is then scrambled and encrypted using a single-use strong key. Even if another application were to "snoop" a VIVIDESK client-server authentication package, it would need to decrypt the container, reassemble and remove redundant digits, then further decrypt the reassembled message... all this in a 128bit encrypted secure socket layer.

How are users authorized?

What categories of authorization are supported?

User authorization is managed by top-level VIVIDESK administrators, who set the authentication options for user access, build desktops for each user group, and configure how information resources and/or software applications will be launched within a desktop context.

The following user rights can be managed with VIVIDESK administrator software:

- Desktop membership
- User group membership
- User Interests
- User logon identifier, access start date, access end date, audit trail, communications tools and desktop preferences
- Software access, Single-Sign-On privileges, context management identity and rights.

- Internet domains where VIVIDESK can be used and/or cannot be used
- Methods of launching software applications
- Requirement for encrypted communications (SSL) for all data exchange between VIVIDESK client and server
- Electronic mail, diary, inventory, discussion group access
- Home page dashboard and usage data access properties

Can security be set at the individual user level?

Security can be set at the individual level as well as at the group and application level.

Security features, such as the ability to change passwords, can be applied differently at the user, user group, and workstation levels. When VIVIDESK is run as a Windows shell replacement, it offers advanced security features that can restrict, for example, access to applications that view network resources.

VIVIDESK security is layered on top of Windows security and serves to "tighten up" overall security with methods that control which applications – on local machines, on networks, on the Internet and via legacy systems (terminal emulators) – users can access and how.

Can the system assign users to roles or groups, and assign security at that level?

Users are assigned a combination of "Group" and "Interest" attributes that determine their rights and roles.

Group membership determines what information and software applications members can access, what messaging system they use, how online tips, reminders, alerts and on-line training will function, whether they can use VIVIDESK document management features, how they access private discussion groups, what level of control they have in a personal diary and whether they can, for example, change their password.

Within groups, users can have one or more "Interests" assigned. These can open up access to additional resources that are approved for the group but are not shown to everyone by default.

Exclusions from specific rights can also be defined at the level of the group or individual.

Can administrative roles be delegated to different groups?

Four classes of administrators are supported:

1. **Master administrators** can edit all desktop, user, user group, software and communications attributes,
2. **Communications administrators** can edit the properties of communications tools (messaging, knowledge inventory, etc.) but nothing else.
3. **Applications administrators** can register and update software to be accessed through VIVIDESK desktops but nothing else.
4. **User administrators** can register new users, decommission existing accounts, and control the specific applications that users and user groups have access to.

The ability to control users, applications and workstations can be assigned to a master administrator. Each function can also be separately assigned to different administrators. Group administrators can be designated and there can be more than one administrator in each class.

VIVIDESK desktops often provide access to knowledge management databases, contact registries, guideline repositories and other information resources that use the VIVIDESK database engine. Items and groups of items within these registries can be assigned to one or more individuals for low-level administrative powers. This ability to delegate responsibility for a specific collection of references, for example, can be extremely useful in distributing the work of maintaining a rich information space.

Can users change their passwords?

If a VIVIDESK user group is authorized for password changes, then a security icon appears at the bottom right of the desktop and users can click there to change their password. Even if a user has the right to change a password, the desktop can be configured to not allow this in specific locations. This use of workstation profiles can prevent password manipulation in public places where user data entry could be witnessed by others.

If desktop users have been granted the right to manage logon identifiers and passwords for specific information resources, they can do this using the same encrypted password management technology.

If complex password rules are enforced, then users can only change passwords in compliance with the password longevity, case, length, alphanumeric and special character rules defined for their desktop.

Can users be reminded about forgotten passwords?

If VIVIDESK is the source of truth for user authentication (as opposed to an external LDAP or Active Directory), and VIVIDESK is configured to support user registration, then VIVIDESK also supports a password reminder system.

When registering, or when later changing passwords within a validated VIVIDESK session, users can select a security question and a secret answer. If they later forget their current password, they can enter their user name in the desktop logon panel, then click on a link for password reminders. This activates a SSL (128 bit encryption) connection to a page where they must select the correct security question and enter a precisely correct secret answer. If this is done correctly, then an email password reminder is sent to the users registered email address.

If complex password rules are enforced with frequent enforced password changes, this feature can dramatically reduce password-related help desk calls.

Is there complete independence between user and workstation?

Yes. The user "takes" their desktop with them wherever they go in an institution, a region, or the Internet at large. This means that a user will always experience the same look-and-feel, with all their personal preferences and shortcuts, wherever they go irrespective of how Windows or Internet Explorer has been configured on a particular machine. Since accounts are managed server-side, a user can sign on at any workstation in the network and get the same functionality. If a particular software application is not available at a particular location, VIVIDESK will not show its icon at that location.

VIVIDESK has a "sleep" mode. Users can elect to "sleep" the desktop instead of closing it when they log off. The next time they log on, on the same computer or elsewhere, the desktop opens and then automatically logs on to every application that was open when the user last logged off. Additionally, the "state" of most applications is remembered, so they are restored to the specific window, frame or web page last active when

the user logged off. VIVIDESK can also be configured by users to "autostart" one or more favorite applications, irrespective of whether sleep mode is used.

All information about the user's desktop is stored server-side, protected by all the database and other security layers invoked server-side. VIVIDESK clients do not use cookies and do not store any local record of web or application activity.

How are communications protected?

How are messages encrypted?

VIVIDESK allows basic and advanced communications encryption at a variety of levels:

- **Client-server communications**

A VIVIDESK project can be configured to only allow client-server communications over a secure socket layer (SSL, 128 bit encryption). This is the default mode for any desktop using single-sign-on capabilities. If in force, then the server will only listen for and accept client communications over the secured channel.

Over and above communications protocol security, VIVIDESK encrypts all application logon information before sending data to its client. The client uses a proprietary VIVIDESK decryption module to decode this information before use client-side. The information is never recorded to disk, cookie, or any other form of temporary data storage.

With VIVIDESK series 5.5 and later, yet another layer of encryption is added. All communications between client and server (not just logon information) are converted to a unique digital format and then encrypted with a complex unique encryption key. The client decodes this information before using the contents and proceeding with further decryption.
- **Inventory access**

A VIVIDESK inventory (databook) can be set to allow access to databook contents only via an SSL/https secure connection (128 bit encryption).
- **SSO parameter communications**

User names, passwords and logon parameters used to support single-sign-on to multiple applications are sent from server to client over a secure Internet connection (128bit). In addition, VIVIDESK further encrypts all personal identifiers and passwords using proprietary cryptography, pools and scrambles the results, converts to a non-alphanumeric format, then encrypts the results using a secret 32-bit key that is never repeated.
- **User account registration communications**

VIVIDESK can be configured to allow users to register for a desktop account using an Internet registration page. This page cannot be viewed except over SSL and user-provided passwords are further encrypted before transmission to the VIVIDESK server. When approving account requests, VIVIDESK administrators can see the proposed account user name. Passwords cannot be viewed, by anyone including the user. The only way for a user to be reminded of a password is to correctly supply both a pre-selected security question and a secret answer.
- **Messaging communications**

S-MIME is supported for secure messaging communications.

Although VIVIDESK can be run over a non-SSL internet connection, the option to require SSL for any client-server communications and the use of supplemental VIVIDESK key encryption methodology ensures an extraordinarily high level of security for all SSO attributes of a VIVIDESK desktop and installation.

Additionally, it is possible to exclude any application from VIVIDESK SSO and to require users to directly enter user names and passwords to those applications.

How are passwords protected on VIVIDESK servers?

There are multiple levels of protection for passwords and certain other sensitive information stored on VIVIDESK servers:

- **Password access**
Although master and user administrators can reset user passwords, the actual passwords are hidden, encrypted and masked such that password characters can never be seen. Therefore, setting new passwords or changing existing passwords are the only ways for administrators to influence the password-allocation process. Most desktops are set up with automated user registration where users declare their passwords outside of any interaction with administrators and the password is never known to anyone other than the user.
- **Database differentiation**
Information about VIVIDESK user access rights and logon identifiers are kept in a database separate from contact lists, usage logs and user diary contents.
- **Database protection**
The databases used to store VIVIDESK logon identifiers and passwords are themselves password protected.
- **Field protection**
The database design is password-protected. Fields that contain passwords are masked.
- **Password encryption**
In addition to encryption that occurs at the level of SSL, VIVIDESK uses a proprietary algorithm to further encrypt passwords before they are transmitted over SSL from server to client.

How are passwords protected on VIVIDESK clients?

VIVIDESK gathers single sign on information from its server at logon time, using all the protections described above. The logon parameters remain available to the client for the duration of a VIVIDESK session. They are stored in a protected area of computer memory, in an encrypted state. None of this information is stored to hard disk, logs, temporary text files or cookies and all information is erased from computer volatile memory when VIVIDESK sessions close (including all web trails whether SSL or non-SSL).

Does VIVIDESK support RSA, Entrust and other security products?

VIVIDESK is a thin client that executes on the user's workstation; communicating VIVIDESK-encrypted information to and from the VIVIDESK server over a SSL (128bit) encrypted Internet connection. To the extent that Vividesk is a program on a Windows machine, it can make use of additional security services and capabilities enabled for that workstation. For example, VIVIDESK has been launched following user authentication with biometrics, identity cards, RSA identity fobs or other methods of opening applications or virtual private networks.

Companies like Entrust and RSA produce a number of security products that can be used to serve a wide range of needs. These include:

- User authentication products
- Encryption for secure transmission of different information types

- Approved automated client software installation
- Digital certificate management
- Digital signature adjudication

Entrust Direct, for example, is used to securely access an Internet web server. An Entrust Direct Client component is installed on the client computer and this is used to manage a user authentication dialog. Once the user is authenticated, the local computer Internet browser is launched and connected to the secure web server, with encrypted transmission through the Entrust Server Proxy. This same product can be used to authenticate users and then load a specific VIVIDESK desktop and user profile, in place of the Internet browser. The VIVIDESK desktop is configured to route all communications through the Entrust Server Proxy (using the /I command line parameter). In this way, the Entrust product is used to fortify authentication to a VIVIDESK environment which then streamlines communications with the secure web server, and also manages other non-secure information services that do not need to go through the Entrust server. Digital signatures and non-repudiation logs are part of Entrust Direct. These complement VIVIDESK functions. **RSA** authentication products can be used in similar ways.

The VIVIDESK system design is very flexible. It can accept third-party "plug-ins" and ActiveX controls and can control these for VIVIDESK purposes. In this way, Entrust or RSA certificate support can be added to the VIVIDESK environment. These more advanced security implementations may require custom configurations from VIVIDESK Global, which has many years of experience with the security needs of health care organizations.

What firewall ports are required for encrypted communications?

VIVIDESK requires only port 80 to be open for the Internet desktop to work. FTP and other internet communication protocols are not used.

It is possible to build VIVIDESK desktops that use a wide variety of Internet technologies. If, for example, the VIVIDESK options for running either Remote Desktop Protocol (Windows Terminal Server Advanced Client) or the Citrix ICA protocol are active, then applications that use those technologies will work within VIVIDESK only if the requisite ports (i.e., 3380) are open on any firewall between the VIVIDESK client and the relevant server computer. Of course, if these ports are closed then neither RDP or Citrix ICA will work outside of VIVIDESK either.

Similarly, if VIVIDESK virtual classroom streaming video, chat or internet conferencing services are used, each may require certain ports to be open on institutional firewalls.

Can records of conventional Internet communications be cleared?

Any application viewed or integrated using VIVIDESK can be forced to use the https (SSL) protocol for encrypted communications.

Many health information applications are web-based (Internet) applications. These make use of Internet communications tools built in to the Windows operating system. One function of such tools is to allow users to browse backwards and forwards in a "history" of pages or sites visited with the Internet application. Such browsing cannot happen without Windows keeping a (carefully hidden) record of Internet locations (URLs) visited. Security breaches can occur if ill-intentioned hackers explore these logs and interpret their meaning.

VIVIDESK includes a setting that can be activated to force all such logs to be destroyed, irrespective of the the application that started them or the web caching settings of the user's default Internet browser. This fortifies the Desktop's "zero-footprint" capability.

How is security verified?

How is authentication integrity verified?

Once a successful user authentication has occurred, a "session key" is generated by the VIVIDESK server. This certificate is a digital combination of unique numbers derived from the client workstation, server, universal time, and a random number. The key is universally unique and can never be repeated.

A VIVIDESK session, once established, is good for a specific user, workstation, server and desktop. No communications between client and server are allowed without a valid key. The key is also required to gain access to any software applications made available through the VIVIDESK desktop, to make use of single-sign-on features, and to communicate with other users.

The veracity of the session key is checked during a server "ping-back" to the client. The ping interval can be customized but defaults to every 5 minutes. If the client session on the specific hardware has not been maintained, or the client fails to "check-in" within the specified ping period, then the session key is deleted and no further communications or information access is allowed between client and server. If software applications launched through VIVIDESK are configured for VIVIDESK authentication, then they cannot be used if a VIVIDESK desktop loses its authentication status. In this way, VIVIDESK differs from most other Internet technologies: the client must re-verify its authentication in order to continue use of information services.

Can time-outs be set to prevent non-authenticated viewing?

VIVIDESK can automatically log off and systematically close all open software applications (launched through VIVIDESK). The time-out period can be set to any number of minutes or it can be disabled and this can be set differently for different workstations and environments

The ability to close both VIVIDESK and any other open software, whether accessed over a LAN, Intranet or Internet and irrespective of the software type (Windows, World Wide Web, Citrix, VT220, etc.) is an exceptionally powerful security feature. The most common security breaches result from users leaving a computer with private applications open on the computer.

How is non-repudiation enforced?

What non-repudiation methods are used?

VIVIDESK can be optionally configured to capture detailed information about how software applications are used, right down to the mouse-click and keyboard input level. Auditing can be turned on or off at the level of users and software applications.

With all auditing features enabled, the state of any change to server database contents (user information, applications information, inventory, discussions and notes) is recorded by capturing the state of the record before and after the change. All changes are linked to specific individuals, workstations, desktops, and clusters of software applications. This auditing data is kept in a distinct database that can be physically separated from user and application databases.

What audit trails are available?

VIVIDESK has extensive data collection capabilities. These include:

- Records of all online help requests and feedback to administrators.
- Optional logon and logoff queries that can ask different questions of different user groups.
- Full featured, automated, multimedia survey tools that can record users' needs and preferences at baseline and at pre-defined intervals.
- Database logs of where and when any system access occurs.
- Automatic recording to databases, real time, of detailed information about user information behaviors including which software is used when, where, by whom and for how long.
- VIVIDESK allows many software programs to be open simultaneously but it records use only of those that have "focus". The records indicate what software was opened, when, where and in what informational context. Keyboard and mouse events can be captured and recorded, allowing deductions about exact uses of particular software packages.
- Automatic recording of all Internet activity triggered by one or more applications, including all Internet sites visited and any keyboard input.
- Logs of all automated workstation updates and any workstation configuration changes.

Auditing can be completely disabled, can be universally enabled, or can be selectively implemented for software applications that should be audited but do not have their own audit capabilities.

Can the audit capabilities be configured for different types of users and applications?

Data collection and audit features can be configured for groups, users, applications and workstations.

Usage monitoring, automated surveys and Internet logs can be turned on or off for entire user groups. Within a group, particular individuals can be excluded from data collection.

One or more applications can be excluded from usage monitoring. Within applications, monitoring of keyboard and mouse events can be turned on or off, as can monitoring of application-triggered Internet activity.

Can the audit capabilities be configured to exempt some items from audit?

VIVIDESK can audit all Internet communications between any VIVIDESK-launched application and that application's server or any other Internet server. These auditing capabilities are powerful and, as previously described, can be turned on or off at an application, user, group or desktop level.

In addition, VIVIDESK can be configured to exempt certain classes of communications from audit. For example, it may be desirable to audit a specific application but skip any record of communications using the https protocol. VIVIDESK can exempt protocols from audit.

Finally, even when all communications protocols are audited, it may be inappropriate to audit specific information exchanges with specific web pages, such as a logon page. VIVIDESK can exempt any page or pattern of pages from audits.

Security Threats

How does VIVIDESK address Internet security threats?

The **Open Web Application Security Project** (see <http://www.osasp.org>) identifies a number of critical web application security vulnerabilities. VIVIDESK has been designed to address all of these, taking advantage of the VIVIDESK non-browser communication channel to overcome serious browser-related vulnerabilities. The 10 top vulnerabilities are addressed as follows:

- **Unvalidated Input**
Vulnerability: Information from web requests is not validated before being used by a web application.
Solution: VIVIDESK server accepts only communications that originate from its client, using a unique key validation method and client signature.
- **Broken Access Control**
Vulnerability: Restrictions on what authenticated users are allowed to do are not properly enforced.
Solution: VIVIDESK re-validates its session credentials with a "push-ping" from client to server at regular intervals, without user input. The desktop sets user rights and manages internet session variables associated with those rights.
- **Broken Authentication and Session Management**
Vulnerability: Account credentials and session tokens are not properly protected.
Solution: VIVIDESK does not rely on Internet server/browser session variables or cookies. It uses its own uniquely encrypted session identifiers and re-validates these at set intervals, including automated destruction of session keys and rights if the correct client signature is not recognized.
- **Cross-Site Scripting Flaws**
Vulnerability: The web application can be used as a mechanism to transport an attack to an end user's browser.
Solution: Since VIVIDESK itself does not use the Internet browser, and the server refuses all requests that do not arise from a specific authenticated VIVIDESK client, this vulnerability does not exist for VIVIDESK. It could exist for a third-party application that VIVIDESK provides access to.
- **Buffer Overflows**
Vulnerability: Web application components written in some programming languages can be crashed and used to take control of a process.
Solution: VIVIDESK has been specifically designed to prevent this. It runs in protected server memory space, isolated from other Internet Information Server processes.
- **Injection Flaws**
Vulnerability: Attackers embed characters in web form submissions that can "fool" an application into executing an unwanted database command (SQL query or process).
Solution: The VIVIDESK server does not accept user-input that is incorporated in SQL statements, and is designed to prevent this vulnerability.
- **Error Handling**
Vulnerability: Attackers cause errors to occur and then learn how to interfere with an application by interpreting error messages that are returned.
Solution: VIVIDESK has been programmed to always return a single generic error message in the

event of any malfunction. It self-restarts and stores all error messages in protected server-side space available only to system administrators.

- **Insecure Storage**

Vulnerability: Weak cryptography can make sensitive content available to snooping internet tools.

Solution: VIVIDESK does not use Internet browser history logs or communication channels or sessions for its client-server communications. Freed of the burden of full Internet browser http request formatting, VIVIDESK can implement strong cryptography that VIVIDESK is specifically designed to handle quickly and efficiently.

- **Denial of Service**

Vulnerability: Attackers can flood a server with requests to a point that legitimate users cannot get access.

Solution: VIVIDESK tracks from where the user is trying to connect using the originating computer's MAC number, instead of IP number (which can be spoofed). If VIVIDESK detects that multiple inappropriate calls originate from the same computer, then it will not allocate new resources for that call.

- **Insecure Configuration**

Vulnerability: Having a strong server configuration is critical to a secure web application.

Solution: This vulnerability is not directly related to VIVIDESK technology. It reminds us that, no matter how good application security may be, if the computer hosting the internet component is not secured, then the component is not secure. VIVIDESK single-sign-on capabilities should not be used unless the VIVIDESK sever and its authentication database(s) are properly secured in a network and physical environment that meets appropriate security technology and policy standards.

VIVIDESK series 5.5 includes many security enhancements that directly respond to these web application security threats. More importantly, VIVIDESK programmers carefully monitor OSASP alerts and pro-actively enhance the client technology to address new threats. The VIVIDESK automated update system can be used to ensure that VIVIDESK servers only respond to updated clients; allowing for automated system-wide correction of any future, as yet unknown, security vulnerabilities.

Single Sign On

Can multiple applications be controlled through a Single Sign On (SSO)?

VIVIDESK goes beyond most Single Sign On (SSO) products by facilitating controlled access and automated procedures (macros) not only for local area network applications, but also for any application running on the client computer or any Internet, Telnet or Terminal emulator application initiated by the client computer.

VIVIDESK has many features that facilitate automated logon to multiple software applications. In addition, the VIVIDESK integration experts can work with organizations and software vendors to produce customized sign-on modules, using VIVIDESK's extensive macro and scripting language, for logging on to particular products and providing users with a wide range of custom shortcuts and productivity aids.

SSO is available for local Windows applications (software running on the client computer) remote Windows applications (Citrix, Remote Desktop Protocol), TELNET/VT100/VT220 sessions, Internet applications, XML and Java applications. NT challenge, querystring, form element, command line, CCOW and other SSO protocols are supported. Additionally, VIVIDESK can reproduce combinations of keyboard and mouse events to support SSO scripting of legacy or other products that do not support SSO protocols. The desktop can automate log-on to Terminal Server sessions and can manage software applications run on remote computers via terminal server sessions.

VIVIDESK can register multiple logon identifiers, passwords and parameters for each user. Application startup and scripting options allow these parameters to be used in a variety of ways to gain access to multiple secure applications. Tokens are used to prevent any recorded or viewable instance of a user identifier or password.

VIVIDESK has a full-featured macro language that can emulate any combination of keyboard, mouse or special key combinations for controlling any type of software that can be launched from the VIVIDESK interface. All SSO procedures are encrypted, with no representation of either the logon technique or content on the client computer.

How does VIVIDESK SSO work?

VIVIDESK has a number of embedded technologies and protocols for facilitating a single sign on to a desktop followed by seamless access to multiple password-protected information resources. Examples include automated user authentication, form-based logons, CCOW application-to-application authentication, and scripted logons. The VIVIDESK SSO scripting language can send user authentication information to any Windows, Internet, telnet or Remote Desktop Protocol software application. In this respect, VIVIDESK is a

SSO toolkit that can be used by desktop designers to construct a single sign on information environment. Specific technologies are best understood through demonstration.

Frequently performed tasks, in Internet, Windows and Remote Desktop applications, can be automated with the use of VIVIDESK macros. These macros simulate user information behaviours and extend the functionality of SSO by allowing applications to be opened and then pre-configured to meet the needs of specific users. Macros can be embedded in education panel abstracts and other HTML pages and forms.

Windows, Internet and Remote Desktop applications can be configured for automated sign on either with Administrator-provided logon names and passwords or with parameters provided and managed by users. It is important to distinguish between VIVIDESK SSO technologies and Internet Desktop policies that can be implemented with VIVIDESK. Irrespective of VIVIDESK capabilities, administrators may decide that they do not want some or all users to have the ability to automate access to multiple applications.

What SSO methods are supported?

VIVIDESK can automate sign-on to software applications by a number of different methods. The methods must be specifically invoked by a system administrator. The default behaviour of a desktop is to not support SSO unless explicitly permitted to do so. Supported SSO techniques include:

- **NT challenge/response:**
VIVIDESK can respond to a standard NT challenge/response over TCP/IP. VIVIDESK uses tokens to manage the user name and password, avoiding any local representation of this information.
- **Internet Querystring or Form-based authentication:**
For applications that use any type of form-based user logon (POST method), VIVIDESK can be configured to emulate the form and pass the user name, password and up to 6 additional parameters.
- **Algorithmic authentication:**
Some applications execute a unique (usually mathematical) algorithm or transposition to determine whether a user name and password will be permitted for submission to the server application. VIVIDESK can be configured with vendor-provided code to execute such algorithms in support of authentication.
- **Component authentication:**
Some applications only accept authentication challenges that are "signed" by a specific encryption algorithm that can only be generated by compiled code that must be registered and incorporated into the client application. VIVIDESK can "contain" such components and use them in support of SSO.
- **Internet address authentication:**
Some applications verify that an authentication request comes from an Internet session opened on a specific server computer. VIVIDESK has the ability to "push" information into such sessions in order to comply with this protocol.
- **Remote Desktop Logon:**
VIVIDESK can pass user names, passwords, and domain names directly to Windows Terminal Services computers, and so automate logon to Windows sessions remotely.
- **Telnet challenge/response:**
VIVIDESK can respond to telnet (VT100) user name and password queries, providing user information and so automating logon to legacy applications.

- **FOB-based Logons:**
VIVIDESK can be scripted to acquire serial number strings from users with security FOBs and use this information to guide a pre-determined logon protocol.
- **Scripted Logons:**
If none of the above methods work, VIVIDESK can send keystrokes, mouse events, clipboard contents and special key combinations to any application that can be displayed in VIVIDESK, irrespective of the software type.

Can the choice of SSO method be context-sensitive?

Yes. VIVIDESK can "sense" the network environment that it finds itself in when a user wishes to log on to a particular information application.

The network environment can be determined by "internal appearances" (how the client network location appears to a local network) or "external appearances" (how the client network location appears to the Internet at large). This information can be used to determine which SSO protocol to use to facilitate access to a information resource. The Desktop user need never know that a stronger method is used outside a protected intranet, for example.

Which hardware and software platforms support SSO functions?

VIVIDESK can automate logons and run automated scripts and macros for the following software types:

- Any legacy system accessible using terminal emulation (VT100, VT220)
- Any 16 or 32-bit Windows software application, either launched from the local workstation or launched over a network (local, wide or virtual private network)
- Any application that can be viewed in an Internet Browser (all Internet Explorer 4.0 or later functions supported)
- Microsoft Windows Advanced Terminal Server client (the client component of advanced terminal server is built-in to VIVIDESK and can be fully controlled and scripted; making VIVIDESK an SSO solution for Microsoft's Remote Desktop Protocol)
- Citrix MetaFrame ICA client for Windows Terminal Services

The VIVIDESK interface for setting up applications is similar to the Windows procedures for setting up software icons, except that administrative work instantly takes effect for an entire network, independent of workstation reboots.

Can VIVIDESK automatically close applications that it has opened?

VIVIDESK can close any software application that it has opened. This includes local Windows applications running on the user's workstation, Windows applications running remotely over the Internet using either

Microsoft Remote Desktop Protocol (Terminal Server Client) or Citrix ICA clients, VT100/220 applications and any Internet application. All secondary windows spawned by Internet applications are also closed.

This is an administrator-configurable feature. Desktops can be set to leave applications open, to close applications without requesting permission from the user, or to close applications only after first checking with the workstation user.

VIVIDESK can be configured to automatically initiate a logout protocol if there is no mouse or keyboard user activity within a configurable time period. If, for example, timeout is set to 4 minutes, then absence of user activity in 4 minutes will result in a brief warning after which VIVIDESK will force closure of every application that it opened. Since these applications could contain sensitive information, this is a powerfully protective "reverse SSO" capability.

Most importantly, VIVIDESK supports "**Single Sign Off**" to complement its "**Single Sign On**" capabilities. This capability is unique, and a uniquely powerful security feature. Many private Internet sites have features that "clean up" after a user interaction, including the erasure of Internet cookies or session variables that could be pried by a malicious user. VIVIDESK prevents this by forcing application specific logoff protocols, even though the user may forget to do so.

Are SSO capabilities limited by firewall, dial-up or web-access constraints?

VIVIDESK runs on top of standard networking protocols. It does not host unique network protocols and is able to conduct all its work over firewall port 8080 (80). This port is almost always open because, without it, the World Wide Web cannot be seen. Nothing more than port 80 and, optionally, SSL (https) is required for a fully functional SSO capability in VIVIDESK.

VIVIDESK has been tested in Windows, Novell and other network environments with proxy and firewall products from various vendors. Firewall and other barriers may limit access to particular domains or types of network traffic in particular environments. VIVIDESK can be configured to use local proxy servers and firewall products.

To what level can an administrator script into an application?

VIVIDESK has multiple methods of achieving SSO functionality. It can automatically respond to a NT user authentication challenge, can automate access to restricted web sites, and can directly interact with Windows Terminal Servers to initiate and control Windows applications running in an Application Service Provider (ASP) environment.

The most versatile SSO method in VIVIDESK is its ability to emulate mouse, keyboard and function key events. This allows VIVIDESK to manage SSO capabilities for a wide range of legacy and current software products because VIVIDESK does not require the software applications to adhere to a SSO protocol.

VIVIDESK supports a variety of "tokens" that can be used to send information from VIVIDESK user databases to applications during their initiation. This means that VIVIDESK can combine information provided dynamically by the user with any information known to VIVIDESK in its databases.

Remote Windows Applications

Application Service Provider Technologies

Overview

The VIVIDESK system is optimized for running and managing Windows applications over the Internet. This means that a software application that normally runs on a Windows computer, including any Internet applications, is executed on a server computer but viewed on a distant client computer. The client sees the expected graphical interface to the Windows application and this interface is continually updated over a communication between the client and the server computer. The Windows application runs on a "virtual workstation" on the server computer and the client is able to remotely interact with this virtual computer.

Citrix Metaframe, Microsoft Terminal Server Client and VIVIDESK all permit Microsoft Windows applications to run remotely over the Internet. All three require that Microsoft Windows NT Terminal Server, Windows 2000 or a Windows 2003 Server be running on a server computer where the Windows applications are installed and configured.

Organizations wishing to support remote windows applications over the Internet often use Citrix MetaFrame or Microsoft Terminal Server. The following questions explore common queries about how these technologies work and how VIVIDESK makes them work better.

Citrix Metaframe

Citrix Metaframe can deliver the graphical interface of Windows applications from the Server computer to the Client. To do this, it needs:

- **Server Side**
An Internet server computer running Windows 2000 or Windows NT Terminal Server Edition with Terminal Services licensed and activated. Citrix Metaframe Server software.
- **Client Side**
A client computer connected to the Internet. Citrix ICA Client software installed on the client.

Microsoft Remote Desktop Protocol

The Microsoft NT 4 Terminal Server, Windows 2000 or Windows 2003 server can also deliver an application remotely from the Server to a remote client computer. This is done over the Internet using the Microsoft Remote Desktop Protocol (RDP) to manage the communication between client and server. RDP needs:

- **Server Side**
An Internet server computer running Windows 2000 or Windows NT Terminal Server Edition with Terminal Services licensed and activated.
- **Client Side**
A client Windows computer connected to the Internet.
Microsoft Terminal Server Client software installed on the client.

VIVIDESK

VIVIDESK is a "container" technology that can hold and control either Citrix clients or Microsoft RDP clients within its shell. The RDP client is built-in to VIVIDESK and so VIVIDESK can run Windows programs over the Internet without need for installation of any additional client software. To run Windows programs remotely, VIVIDESK needs:

- **Server Side**
An Internet server computer running MS Windows 2003, Windows 2000 or Windows NT Terminal Server Edition with Terminal Services licensed and activated.
- **Client Side**
A client Windows computer connected to the Internet.
VIVIDESK client installed. The client is the same software as used for all other VIVIDESK functions.

Can VIVIDESK be used as a thin-Client for Citrix and Microsoft Servers?

Given a Citrix Metaframe server or a Windows Terminal Server, VIVIDESK can serve as a thin client in one or more of the following ways:

- **ICA (Citrix) Client Manager for Citrix Server**
The ICA client is used to establish a connection with a Citrix server computer and to run Windows applications over the Internet. The ICA client software works within VIVIDESK. VIVIDESK can run multiple ICA sessions, facilitate communication among those sessions, economize on the number of user licenses required, and automate logons and shortcuts within multiple ICA client sessions.
- **Advanced Terminal Server Client Manager for Terminal Server**
The Advanced Terminal Server Client uses Microsoft's Remote Desktop Protocol (RDP) to establish a connection with a Windows Terminal Server computer and to run Windows applications over the Internet. VIVIDESK has an embedded RDP viewer. VIVIDESK can run multiple RDP sessions, facilitate communication among those sessions, economize on the number of user licenses required, and automate logons and shortcuts within multiple RDP client sessions. ICA and RDP sessions can be run simultaneously and can share information via the VIVIDESK container.

- RDP Client Manager for Citrix Server**
 The VIVIDESK RDP client is compatible with the Citrix server. This client software has some potential advantages over the ICA client for Windows workstations. VIVIDESK allows either the RDP client or the ICA client, or both, to be used in conjunction with a Citrix Metaframe Server.

VIVIDESK does not need Citrix software to be present on either client or server computers. If Citrix software is installed server-side, VIVIDESK can take advantage of its features, either for application management or by using its ICA client.

How do Citrix, RDP and VIVIDESK technologies differ?

The Citrix ICA client and Microsoft remote access ActiveX control (Advanced Terminal Server Client, RDP) perform the same functions, with some differences in functionality. The VIVIDESK remote access system includes the Microsoft RDP functionality, adds additional features, and can combine both Citrix and RDP clients in one user interface. To our knowledge, the VIVIDESK version of RDP is the only RDP methodology currently available that supports multi-session, single-sign-on, scriptable remote Windows application control.

Feature (note)	ICA	RDP	VIVIDESK
Client			
Windows 95, 98, NT, 2000, XP compatible	✓	✓	✓
Macintosh, Unix compatible	✓		
Run 16-bit Windows applications over Internet	✓	✓	✓
Run DOS applications over Internet	✓	✓	✓
Run 32-bit Windows applications over Internet	✓	✓	✓
Server Management			
Create user accounts and rights using NT or Win2000 user management		✓	✓
Create user accounts and rights using custom user management software	✓		✓
Set up applications server-side by associating with user profiles	✓	✓	✓
Server-side logon to NT user profile and automated start of Windows application	✓	✓	✓
Client-side automated logon using userid and password from a general person index, either Windows user registry, VIVIDESK registry or third party registry (1)			✓

Feature (note)	ICA	RDP	VIVIDESK
Ability			
Workstation Integration			
Non-dithered full 256 color palette replication, without color distortions irrespective of differences between client and server color palette.		✓	✓
Seamless mapping to client default printer.		✓	✓
Ability to run multiple Windows client sessions, without loss of clipboard, printer or drive mapping functionality. (2)			✓
Ability to run scriptable ICA and RDP interfaces in same graphical interface. (2)			✓
Automatic client-window resizing to match client screen resolution. (3)			✓
Infinite client-window size options. (3)			✓
Full Windows clipboard support. (4)		✓	✓
Local drive mapping so that client drives accessible to server applications	✓	✓	✓
Audio System Beeps		✓	✓
Stereo Windows Audio	✓		
Application Integration			
Support for 6 additional clipboard channels for moving information between Windows applications, remotely managed, even if those applications are on multiple servers. (4)			✓
Simultaneous sign on to multiple terminal server computers, all run on the same client with common printer and clipboard control. (4)			✓
Ability to move data between multiple Citrix and RDP sessions. (2)			✓
Connect directly to applications rather than entire desktop	✓	✓	✓

Feature (note)	ICA	RDP	VIVIDESK
Connect directly to multiple separate applications on one terminal server, using one license.			✓
Single user can access multiple terminal servers and terminal server profiles using different usernames and passwords; full SSO capability. (6)			✓
Logon scripts. (6)			✓
Macro scripts. (6)			✓
Applications can be set to time-out after a period of inactivity.	✓	✓	✓
Security			
SSL (https) encryption of userids and passwords; up to 128-bit cryptography	✓	✓	✓
Additional client-server encryption of terminal server logon parameters, active even if https is not used. (5)			✓
Optional substitution of advanced RSA or Entrust cryptography for protection of logon parameters. (5)			✓
Automated logon to secured applications after Windows NT challenge. (6)			✓
Licensing			
Terminal Server Application Mode licensing required from Microsoft.	✓	✓	✓
Additional Server license required from Citrix		✓	
Seat licensing: one client access license used for each workstation/user combination. (7)	✓	✓	
Connector licensing: any number of users and workstations up to a certain number of simultaneous connections. (8)		✓	✓
User licensing: multiple users can access one or more terminal servers in same server cluster, coming in			✓

Feature (note)	ICA	RDP	VIVIDESK
from any number of workstations, and use up only one CAL. (8)			
Administrators can change all user and application rights and passwords without using up Terminal Server licenses.			✓
Automated client-side time-out irrespective of terminal server time-out settings. (9)			✓
Other Features			
Record of terminal server sessions; number, start time, end time.	✓	✓	✓
Record of activity within terminal server sessions; mouse events, keyboard events, amount of time session has focus. (10)			✓
Record of information exchanged between remote access applications. (10)			✓
Can run on terminal server thin clients; 100% application service provider compatible.	✓	✓	✓
Can run Windows applications on the client side as well, with full scripting, integration, macro, and usage monitoring.			✓
Can substitute for the Microsoft Windows shell and so provide complete workstation "lockdown" with thin-client technology.			✓
Ability to distribute remote desktop requests to different servers, conditional upon network location of the client. (11)			✓
Users can store information from remote desktop sessions in a personal diary that remains part of the user's desktop.			✓

Note	Explanation
1.	The Microsoft RDP ActiveX control (for Internet Explorer) does not allow user names and passwords to be sent to the server by the client shell program (Internet Explorer or some other browser). The RDP control built in to VIVIDESK provides VIVIDESK with full access to all features, including those not enabled for usual Internet

Feature (note)	ICA	RDP	VIVIDESK
			<p>use. Consequently, VIVIDESK can send commands via the RDP protocol. These special communications can include information for automatically logging on to a particular terminal server profile, loading software and controlling such things as screen resolution, clipboard and printer functions.</p>
2.			<p>Because the RDP client is built-in to VIVIDESK, multiple remote Windows applications can be run along side one-another, each protected from the other's memory space but each also able to share information and run under a single graphical interface. To do this using the Microsoft ActiveX control or the Citrix ICA control requires multiple instances of Internet Explorer running, without the ability for these to share session variables.</p>
3.			<p>When RDP is used via the Microsoft ActiveX control in Internet Explorer or via the Advanced Terminal Server Client, a screen resolution must be selected from a limited set of pre-defined resolutions. VIVIDESK is able to set the screen resolution to exactly the amount of space available on the client computer, thus optimizing use of the graphical Interface. The same applies to the Citrix ICA client, which forces a specific screen resolution even if this means wasted space on the client computer. For this reason, remotely managed Windows applications in VIVIDESK look like they are fully integrated into the user interface. They "maximize" to take up all the available screen area.</p>
4.			<p>The RDP client, as contained in VIVIDESK, supports multi-level clipboards and the ability for the server and client clipboard to share information seamlessly. VIVIDESK additionally provides 6 independent clipboard channels that facilitate a total of 7 communications ports between multiple remote-control Windows sessions, even on different servers.</p>
5.			<p>VIVIDESK adds proprietary userid and password encryption to protection offered by the https Internet protocol.</p>
6.			<p>VIVIDESK has the ability to send keystrokes, mouse events, clipboard contents and other information to open ICA (Citrix) or RDP (Windows) sessions. This scripting capability can be used to automate complex logon procedures and to provide users with macros that perform common functions across multiple different types of windows applications running remotely.</p>
7.			<p>Microsoft Terminal Server client access licenses (CALs) are required for both Citrix and Terminal Server remote application delivery models. One CAL is used for each user/workstation combination. This means that if a single user accesses the Terminal Server from three different computers, three CALs are used.</p>
8.			<p>The optional Microsoft Terminal Server Internet Connector license allows 200 simultaneous remote access sessions for a server or server farm covered by the license. In this case, a license is consumed for each workstation, user and connection but the licenses are returned to the pool after the user logs off. A CAL (above) is permanently associated with the workstation that</p>

Feature (note)	ICA	RDP	VIVIDESK
			activated it. The Internet Connector License, however, only covers a single terminal server access user account. The VIVIDESK system optimizes use of the more economical Internet Connector License because it allows many different users, with different privileges, to be using the same license. This fact, when combined with the fact that VIVIDESK setups do not require Citrix licensing, represents a major cost saving.
9.			VIVIDESK's ability to easily assign different automatic sign-off times to different users and user groups, makes it possible to gain all the security advantages of inactivity signoffs without having to set up unique application and user profiles on the server for every possible time-out scenario. This represents a major savings in administrative time.
10.			The Terminal Server management software is capable of keeping detailed logs of what happens on the terminal server computer. The VIVIDESK system adds to this information by having the ability to also record what happens on the client computer. This greatly extends audit and usage monitoring capabilities.
11.			VIVIDESK can associate many different methods of accessing a remote desktop server with a single user. Which server to use can be decided based on the client computer location or other rules. This feature can be used to increase overall reliability of the system.
12.			A Macintosh-compatible RDP client is expected from Microsoft. As soon as this technology is available, it will be added to VIVIDESK.

How do Citrix, RDP and VIVIDESK server management methods differ?

The Citrix server-side software includes advanced user and application management tools. These can simplify "load balancing" whereby a Windows application is available on multiple terminal servers and the client can be directed to the one with the least load at the point that it makes a request of a server in a Citrix neighborhood. This same load balancing functionality can be replicated on a cluster of Windows 2000 servers but requires more know-how of the network administrator. On the other hand, network administrators usually require special training and certification to become adept at managing Citrix server clusters.

Both Citrix and Microsoft RDP configurations use Windows NT user profiles and rights for managing which clients are able to access which resources within a network domain.

VIVIDESK sits on top of either Citrix or Microsoft RDP server-side user and application management. VIVIDESK user and application management tools are easier to use and administer. A common approach is to cut down on the number of NT profiles server side (as few as one or two) and allow VIVIDESK to manage differential user rights within those profiles.

How do Citrix, RDP and VIVIDESK handle licensing and user fees?

Cost comparisons between remote Windows delivery strategies should be based on common feature sets. However, the VIVIDESK system adds many features not available with either Citrix or RDP stand-alone configurations. Therefore, the relevant cost comparison is between Citrix and RDP approaches, with VIVIDESK cost additions or subtractions added to either model.

What does VIVIDESK add to remote desktop services?

Adding VIVIDESK to any of the above scenarios can improve performance and reduce total cost of ownership, even if initial total license costs appear greater. Remote Windows application strategies are most vulnerable to the capacity of the terminal server computer(s). Each remote application causes a "virtual" personal computer to be created in the server memory. Each new user and each new application consumes additional server resources. In this way, as few as 10 simultaneous remote users (and 10 virtual personal computers in server memory) can significantly slow performance. For this reason, Citrix and Microsoft provide methods to balance the load of virtual computers across multiple servers. VIVIDESK can help systems administrators get more out of limited server resources in the following ways:

- Multiple RDP sessions running from a single VIVIDESK session use but one virtual machine.
- VIVIDESK is usually configured to open a single software application on the server, minimizing the resources consumed by such sessions because other Windows components do not have to be loaded.
- VIVIDESK allows many users, with many different VIVIDESK rights profiles to share a single Terminal Server Internet Connector license. This can greatly reduce the number of licenses required to sustain a user group.
- VIVIDESK automatically logs users off terminal sessions as soon as they are no longer needed. This conserves valuable server resources.
- VIVIDESK can distribute terminal server sessions among multiple servers without going through server-side load balancing software. This can significantly reduce the cost of setup and maintenance of a terminal server cluster.

Can VIVIDESK be run on a remote desktop server?

VIVIDESK can be installed and run on either a Microsoft Windows Terminal Server or on a Citrix server. The VIVIDESK client is set to open in a special terminal server compliant mode so that multiple "virtual machines" can co-exist on the same computer server with the same apparent internet address.

Recent versions of both the Microsoft (Windows Terminal Server 2003) and Citrix products support the color depth and audio capabilities expected of many of the software applications run within a VIVIDESK desktop.


Context Management

Does VIVIDESK support context management?

VIVIDESK supports a number of different methods for multiple software applications and Internet resources to share information about the current decision-making context. VIVIDESK includes a context administrator that can be used to register the exact technologies that applications will respond to in a changing information context.

VIVIDESK also functions as a context monitor and manager, aware of changing patient, provider and problem identifiers in other applications, and it can broadcast context changes to applications running within VIVIDESK. This later capability allows VIVIDESK to manage context sensitivity for applications that may not yet be compatible with prevalent context administration protocols.

The wide range of integration and context management capabilities offered by VIVIDESK systems can best be appreciated by demonstration:


 [Click here to launch a video presentation, then select the "coupling" and/or "contextualizing" links.](#)

What context management method is used?

VIVIDESK is fully Context Management Architecture (CMA) compliant, as defined in HL7 Context Management Standards from the Clinical Context Object Working Group (CCOW). It includes a CMA administrator that can be used to register multiple applications and the exact identifiers that each will respond to in a changing information context.

VIVIDESK maintains 5 context clipboards (patient, provider, problem, procedure, policy) and shares the information with all applications opened by VIVIDESK. The scripting language can access and use information in these clipboards and can respond to context-triggered changes in any of the context channels. This means that VIVIDESK can use information from one software application (e.g., a patient identifier), to script into another application. This capability is behind VIVIDESK's "CCOW-Light" context management capabilities, offering context management for applications that have yet to acquire this capability. Scripts can be triggered simply by changing client-side focus from one software application to another. In this way, multiple software applications, based on different core technologies, can be "aware" of and use information from a shared decision-making context.

The complementary abilities of CCOW-Full and CCOW-Light can best be appreciated by demonstration.

 [Click here to launch a video presentation, then select the "CMS-Light" and/or "CMS-Full" links.](#)

Usage Monitoring

How is data collected and what is captured?

Basic information about a VIVIDESK session is always captured. In this way, it is known how many times different users log on to particular VIVIDESK desktops. Basic VIVIDESK session information is stored in the VIVIDESK data server databases.

Further data collection can be turned on or off user by user. The VIVIDESK Administrator software is used to set the data collection properties for each VIVIDESK account. Although the default is "ON" when creating new user accounts, any account can be designated for no data collection. In this case, no information is ever recorded to the desktop database for this account. This feature is useful in conventional and market research. For example, it may be desirable to not record desktop usage by system administrators. If user data collection is turned on, it is still possible to independently prevent data collection about specific software applications.

The VIVIDESK Administrator software is used to set the data collection properties for each registered software application and information resource. If application data collection is turned on, it is still possible to independently prevent capture of keyboard activity. This feature is useful if, for example, there is a need for information about how often an application is used but for privacy reasons it is not appropriate to record what information is entered to that application.

What types of usage data are tracked?

VIVIDESK always captures basic information about VIVIDESK sessions. A session starts with a validated user logon and ends when a user signs off, is timed out, or if the VIVIDESK desktop fails to check in with the VIVIDESK server. Automatic session data includes the desktop requested, user unique identifier, security key, user computer address, logon time, and whether the session ended normally or possibly had a problem.

VIVIDESK optionally captures much more detailed information about exactly how software applications are used within VIVIDESK. Whether this information is stored or not depends upon whether data collection is turned on for a particular user account (if off, no data is captured for that user) and application (if off, user data may be collected but not the particular application data). Optional usage data includes information about how long the user interacted with each software application, what associated websites were visited and what sequence of mouse clicks and keyboard input was used. It is even possible to track how the Internet is used for each Internet-ready application made available via VIVIDESK.

VIVIDESK can record information about who logs on, when, where and for how long. It also can capture much more detailed information about how the VIVIDESK desktop and its software applications are used.

In what format is VIVIDESK usage data recorded?

The VIVIDESK server computers record all VIVIDESK usage data. No usage information, or any record of VIVIDESK activity for that matter, is recorded on the local computer workstation.

Depending on the VIVIDESK server configuration, usage data may be stored in Microsoft Access Tables, Microsoft SQL Server databases, or other SQL database products. Either way, the database content can be exported to a wide range of other formats.

Can audit results be displayed online?

VIVIDESK includes a "DataView" for system administrators. This allows immediate graphical display of system usage data. For example, one could request information about the total duration of use of particular software products by selected user groups during a defined time interval. The results are displayed in various chart formats and can be printed.

The same DataView tool can be used to extract data subsets from the audit records. Extracted data is in Access table format and can be analyzed using standard statistical tools.

Communications

Can global messages be sent out?

VIVIDESK has two embedded messaging systems and it can implement third party messaging systems. VIVIDESK can also associate pop-up messages and summaries with software applications.

The VIVIDESK interface has a "messaging" section to the left of the screen. This can be used to send one or more messages to all or part of a VIVIDESK user group. The messages can change at every log-on and they can be sent out in "bulletin" mode when one message overrides all others and gets distributed to everyone immediately (for VIVIDESK networks and Intranets). Similarly, alerts can be set for only specific user groups. VIVIDESK includes a user-friendly message writing tool that administrators can use to quickly author tips, or use the clipboard to copy them from other software. Tips are formatted in HTML and so can have a wide range of graphical features. They can be linked to help files, Internet resources or to any software package registered in VIVIDESK. Because the tips are entered and edited online, there is no need to upload or modify HTML files on a web server.

What is the best way to add messages and applications?

Applications and abstracts can be thought of as two sides of the same coin. An application is any resource (Internet/CD-ROM/Windows) that is intended for use by project participants. Abstracts are short descriptions of (or guides on how to use) applications. Abstracts are directly associated to applications -- when opened, an application will appear in the right hand panel of the VIVIDESK Desktop, and its abstract will appear in the left hand panel.

Messages (also called Tips) are generally guides for using VIVIDESK features or other topics of interest for a particular group of participants. These (like abstracts) appear in the left-hand panel, however, they are not directly associated with any applications.

A master list of messages and applications/abstracts are kept in **Library**. This is where any new additions should be added using the VIVIDESK TIP template for tips /messages and the VIVIDESK APPLICATION template for applications/abstracts.

Messages and applications can be nested from Library into whatever VIVIDESK Inventory Databook you are working with. Once messages and applications have been added to a Databook it is easy to add them to the associated VIVIDESK desktop using the VIVIDESK admin Message Builder (messages/tips) and the VIVIDESK Application Abstract Builder (applications/abstracts). These builders will guide the process by providing a list of folders or items that contain VIVIDESK TIP or VIVIDESK APPLICATION templates.

Support

What is the level of fault tolerance?

Faults can occur at many levels. VIVIDESK has features that improve the fault tolerance of software applications, client workstations and network connections. The most important fault-tolerance functionality, however, stems from the thin-client nature of the VIVIDESK product. No matter what happens on the client computer, VIVIDESK data files and server performance will not be affected. Other types of fault-tolerance help to decrease the cost of ownership and maintenance of Windows workstations:

- **Application failures**

When a user exits VIVIDESK, or is timed out, VIVIDESK closes all open applications and restores the computer workstation to a clean, simple, state. This alone reduces the incidence of software conflicts and failures. Moreover, VIVIDESK cleans up stray program fragments from software applications that may have failed. This decreases the probability that the software will crash the next time it is initiated. Because VIVIDESK offers a number of configuration options for running software applications, well-tuned VIVIDESK systems often prove more stable than conventional Windows setups.

- **Workstation failures**

VIVIDESK offers a number of strategies for decreasing the likelihood that computer workstations will fail. These include simplified boot-up processes, control over task manager, automatic workstation resets and automated workstation upgrade support.

- **Network failures**

VIVIDESK supports a secondary or backup system in the event of a network failure. If the VIVIDESK client cannot connect to its primary server for any reason, attempts to connect to a designated backup server. This happens even if VIVIDESK has already started. As long as the backup server connects to the same SQL database server, the primary and backup connections will work seamlessly without the user being aware of the failure.

VIVIDESK will continue to work even if there is a complete network failure and all contact is lost to both primary and backup servers. The user will periodically receive a message that there appears to be a network failure. This message is generated each time the VIVIDESK client "pings" its server for acknowledgement. The "ping" interval can be set by administrators: as short as every minute or as long as no pings at all. Internet applications running within VIVIDESK may fail if they cannot resolve hypertext links followed by the user and there is no local cache of the file.

VIVIDESK can be configured to use a "ping" interval that is so long as to allow VIVIDESK to run completely independently of the Internet after an initial connection is made and a desktop presented to the user.

- **Server failures**
Fault tolerance at the level of the server is dependent upon network architecture and network administrator choices. VIVIDESK has been tested in server clusters with load balancing and fail-safe architectures. VIVIDESK has experience with mission-critical systems. At the level of hard drive mirroring or network replication, VIVIDESK benefits from whatever backup and network protections already exist.

What level of support comes with VIVIDESK?

Pilot Projects, Custom Solutions

There are a number of options for support in addition to VIVIDESK's complete online manuals, Internet support files, mailing lists and electronic bulletin boards.

VIVIDESK service groups usually prefer to have a direct relationship with their clients during any demonstration project or proof of concept.

Implementation

VIVIDESK service providers give direct user support during installation and initial implementation of VIVIDESK systems. The goal is to teach support staff so that they have full control over user, application, workstation and data management. At the conclusion of training (usual requirement is 1/2 day), the desktop service provider can package customized auto-installation, backup and data management routines.

In most cases, institutions prefer to be trained to provide Tier I support through their own help desk.

Tier II support can be taught to the client, obtained from a VIVIDESK service provider, or outsourced to VIVIDESK Global.

Tier III support (any malfunction of VIVIDESK software) is provided directly by VIVIDESK Global partners.

Electronic mail and telephone help lines are serviced together with Internet electronic mail lists and newsgroup support that is connected to other VIVIDESK installation centers.

Regional Roll Out

Desktop service providers work with Value Added Resellers and with Systems Integration Support companies for large VIVIDESK installations.