Vergence®

Desktop Components 3.3
Installation Guide

Windows XP,
Windows 2000,
Windows NT,
Windows 95
Windows 98

Sentillion®

Publication number 0900-1007
Version 3.3

Printed in USA

Warranty

The information contained in this document is subject to change without notice.

Sentillion makes no warranty of any kind with regard to this material, included, but not limited to, the implied warranties or merchantability and fitness for a particular purpose.

Sentillion shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Trademarks

Vergence® and Sentillion® are registered trademarks of Sentillion, Inc.

Microsoft, Windows XP, Windows 2000, and Windows NT are either trademarks or registered trademarks of Microsoft Corporation.

This product includes code licensed from RSA Security, Inc.

Some portions licensed from IBM are available at HTTP://oss.software.ibm.com/icu4j.

Citrix® is a registered trademark of Citrix Systems, Inc.

Adobe® and Acrobat® are registered trademarks of Adobe Systems Incorporated.

Sentillion, Inc.
300 Brickstone Square
Andover, Massachusetts 01810
(978) 749-0022
info@sentillion.com

Notice to Government Users

The Sentillion product suite is commercial computer software that includes commercial documentation, manuals, and related technical data. The development of this commercial software was privately funded, with no government funding, therefore, the only rights that the Government has to this commercial computer software are those specified in the applicable Government license agreement. The Software and documentation provided therewith are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government is subject to the restrictions as set forth in Federal Acquisition Regulation 12.212 for civilian agencies and Defense Federal Acquisition Regulation 227.7202 for military agencies.

Vergence Documentation

All Vergence products have documentation in the form of PDF files and Help files on the CD-ROM. The available documentation for the Desktop Components products includes the following:

Title	Document Number
Vergence Context Administrator User’s Guide	0900-1006
Vergence Context Administrator Help	*Installed with product.*
Vergence Desktop Components Installation Guide (this book)	0900-1007
Vergence Context Vault User’s Guide	0900-1028
Vergence Context Vault Help	*Installed with product.*

Contents

1

Introduction to the Vergence Desktop Components

The Sentillion® Vergence® Context Management Solution is a platform for coordinating and synchronizing CCOW-compliant applications at the clinical desktop. These applications are linked together so that they automatically “tune” to the same clinical context, as established by the user’s inputs. The clinical context is comprised of a set of clinical subjects that identify real-world entities, such as a user, patient, or clinical encounter.

This document provides information about Vergence Desktop Components. The Desktop Components consist of the Vergence Locator and the Context Manager Proxy.

Windows System Requirements

The following table summarizes the system requirements of the Desktop Components software in a non-Citrix environment.

Type	Requirement
Windows Operating system	One of the following: • Windows XP • Windows 2000 • Windows NT® 4.0 with Service Pack 3 or later • Windows 98 • Windows 95 OSR2, with the Windows Socket 2 Update
Windows disk space	5.6 MB required for Sentillion software
Windows network connection	TCP/IP
Software (provided on the Vergence Desktop Components installation CD-ROM)	Adobe® Acrobat® Reader 5.0, required for viewing the online version of this document. **Note**: Adobe Acrobat Reader can be downloaded free from the Adobe web site: www.adobe.com.
	Microsoft's Java Virtual Machine `(%windir%\system32\msjava.dll)` Version 5.00.3188 or later. Note: You may use the most recent version. Microsoft's Java Virtual Machine can be downloaded from their website www.microsoft.com/java.

In a Citrix environment, the following changes are required:

Citrix Metaframe Version	Operating System
Citrix Metaframe 1.8, Service Pack 3	NT 4, Service Pack 3
Citrix Metaframe XP, Feature Release 1.0	Windows 2000

Vergence System Architecture Overview

There are two system architecture diagrams. See the diagram “Vergence Context Management System Architecture” on page 1-7 for applications running on the desktop. See the diagram “Vergence Context Management Architecture in a Citrix Environment” on page 1-8 for applications running in a Citrix environment. Both diagrams show the connections among the components and the CCOW-compliant applications that they serve, as well as the various means by which all of these software modules communicate.

A Vergence Context Management System consists of:

- A set of software components that are deployed on each Vergence-enabled clinical desktop, or referenced from a Citrix server,
- Context Vaults for hosting network-based Vergence software services, and
- The Context Administrator and Vault Administrator tools.

Vergence Desktop Components – The Desktop Components enable applications running on a desktop to communicate with the appropriate Context Manager.

- **Vergence Locator** – The Locator provides an implementation of the CCOW-specified Context Management Registry and serves as a COM Mapping Agent bridge.
    - **Context Manager Registry (CMR)** – The Registry enables all of the CCOW-compliant, Web-based applications that are accessed by a user from a particular clinical desktop to obtain the URL for the Context Manager.
    - **COM Mapping Agent Bridge** – The Mapping Agent Bridge determines whether there are any COM-based mapping agents on the desktop, and if so, serves as a transparent network communication bridge between these agents and the Vault hosted Context Manager.
- **Context Manager Proxy** – The Context Manager proxy is used by CCOW-compliant COM-based applications that are resident on the desktop. The Context Manager Proxy is a COM component that communicates

with the Vault-hosted Context Manager over the network on behalf of these applications. The location of the Context Manager is transparent to the COM-based applications.

Vault-Hosted Services

- **Vergence Vault Administrator –** The Vault Administrator lets you configure and monitor the network behavior and operation for your system of Vergence Context Vaults. This tool resides on the Vergence Context Vault and is accessed via a Web browser.
- **Vergence Context Manager –** The Context Manager coordinates and synchronizes applications at a clinical desktop so that they automatically remain "tuned" to the same clinical context.
    - Supports common subjects and secure subjects, as defined by the CCOW standard.
    - Has built-in support for the Patient Link, User Link, and Encounter Link capabilities defined by the CCOW standard.
    - Supports custom subjects and inter-dependent subjects, as defined by the CCOW standard.
    - Supports both Web-based and COM-based applications and mapping agents.
    - Supports enhanced secure, remote administration functions, including configuration, performance monitoring, and diagnostic logging, through the use of the Vergence Context Administrator.
- **Vergence Security Auditor –** The Vergence Security Auditor works in conjunction with the Vergence Context Manager, recording all context-related events on Vergence-enabled desktops in your enterprise and storing these events on a Microsoft SQL Server™ database. Security Auditor centrally monitors and tracks user interactions across multiple CCOW-compliant applications. This component is optional.
- **Vergence User Mapping Agent –** The Vergence User Mapping Agent, specific to the user subject, maps the user's logon name, as known by a particular application, to the other logon names by which the user is also known to the other User Linked applications. The Vergence User Mapping Agent is optimized for use within a Vergence system. However, Vaults may be configured to use a remote user mapping agent that is compliant with the

Health Level Seven Context Management Standard in place of the Vergence User Mapping Agent.

- **Vergence Vault Database –** The Vault Database is an LDAP database that is used for securely storing passcodes, Vergence User Mapping Agent data, and general Context Vault configuration and administration data. You can access this database with the Context Administrator tool, and you can back up and restore it with the Vault Administrator tool.

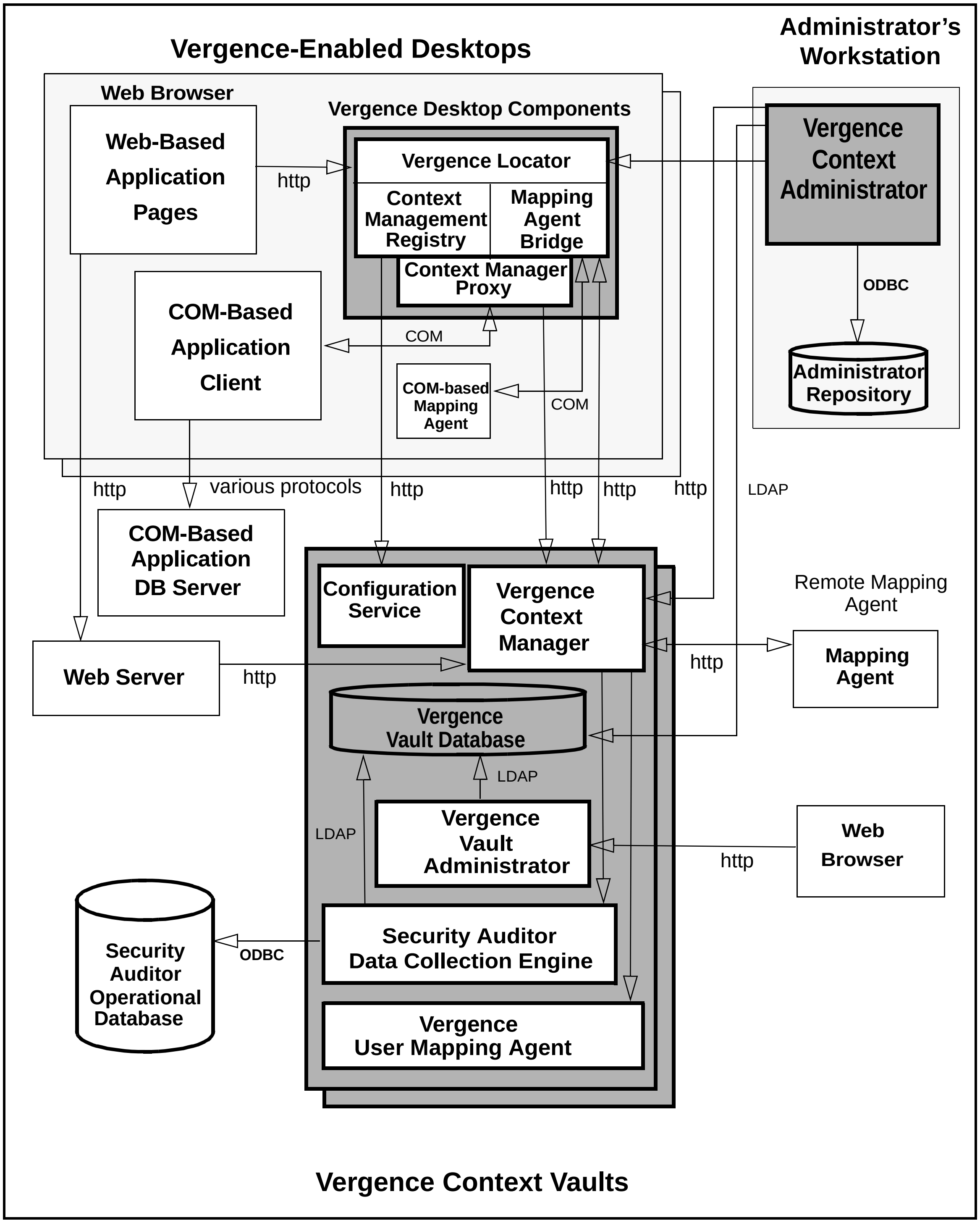
- **Vergence Configuration Service –** The Configuration Service manages site configuration data in the Vault database.

Vergence Tools

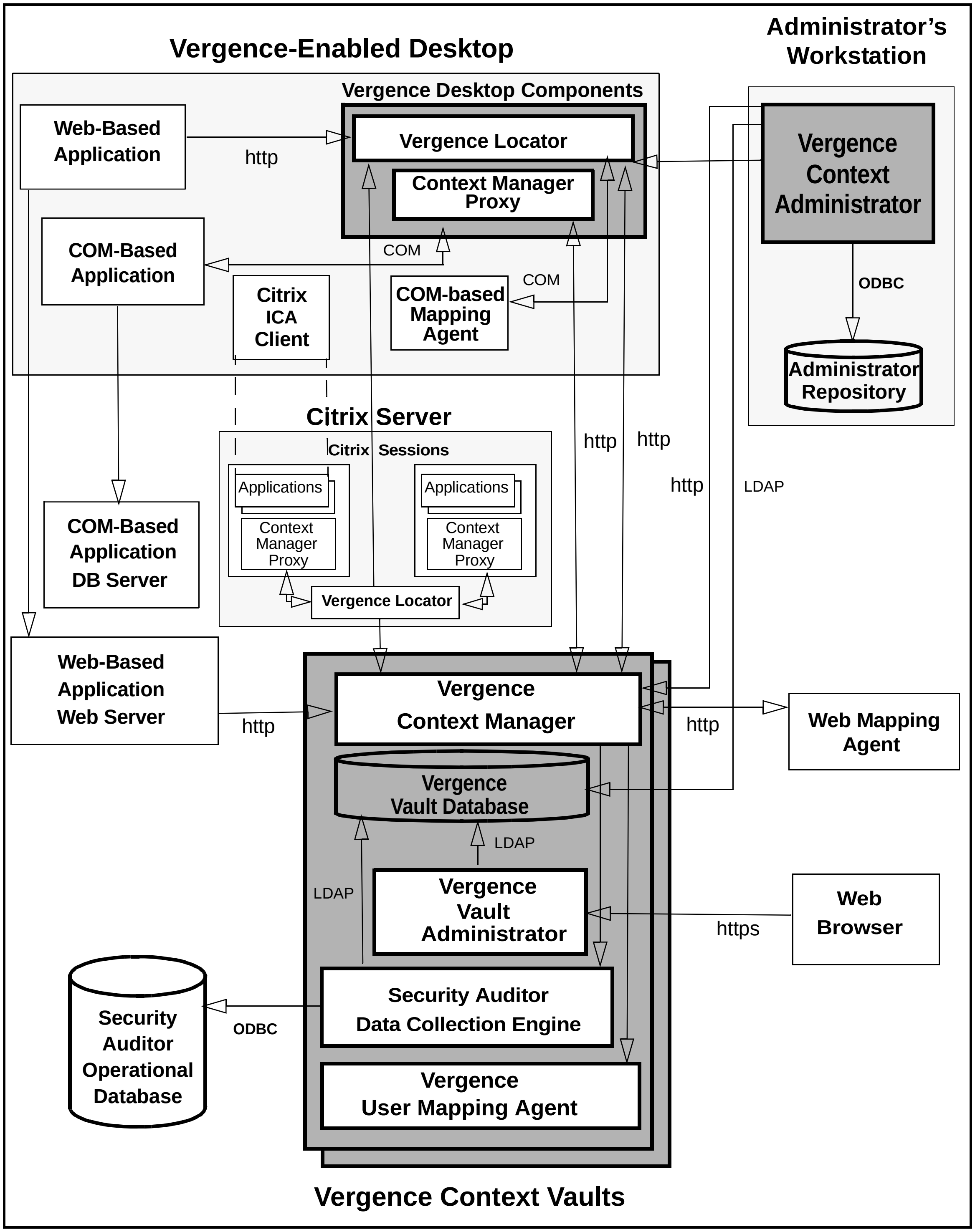
Vergence tools include the Vergence Vault Administrator (discussed previously) and the Vergence Context Administrator. Each of these components has a separate manual to describe its functionality in full.

- **Vergence Context Administrator –** The Context Administrator lets you remotely configure and monitor the context management-related behavior and operation of an overall Vergence Context Management System. The Context Administrator uses the Administrator Repository to maintain network address information about the Vergence-enabled desktops in a system.

The Vergence Context Management System Architecture diagram shows the components that would be used in a production environment.


Vergence-Enabled Desktops
Administrator's Workstation
Web Browser
Web-Based Application Pages
Vergence Desktop Components
Vergence Locator
Context Management Registry
Mapping Agent Bridge
Context Manager Proxy
Vergence Context Administrator
http
COM-Based Application Client
COM
COM-based Mapping Agent
COM
ODBC
Administrator Repository
http
various protocols
http
http
http
http
LDAP
COM-Based Application DB Server
Configuration Service
Vergence Context Manager
Remote Mapping Agent
Mapping Agent
Web Server
http
http
Vergence Vault Database
LDAP
LDAP
Vergence Vault Administrator
http
Web Browser
Security Auditor Operational Database
ODBC
Security Auditor Data Collection Engine
Vergence User Mapping Agent
Vergence Context Vaults

Vergence Context Management System Architecture



Vergence Context Management Architecture in a Citrix Environment

Security

Sentillion provides each site with unique versions of the Context Administrator, Vergence Locator, and Context Vault software that are stamped with a unique internal key. The software uses this key for encryption and signatures and stores the key in a scrambled fashion to avoid being compromised. Therefore, for a production environment, the context management components you received from Sentillion can only interact with other Sentillion components produced for your site.

The Desktop Vault, Vergence Locator, and Context Administrator shipped with the Software Development Kit do not have unique keys for each site. They use a universal set of keys and thus do not provide the same level of security as the components that are stamped with unique keys. For these security reasons the Vergence Locator and Context Administrator shipped with the Software Development Kit will not interoperate with the components installed in a production environment.

Network Considerations

The various components of a Vergence Context Management System must be able to communicate with each other over the network. Some of these communications are specified in the HL7 CCOW Specification and some are proprietary to the Vergence Implementation.

The diagram “Vergence Network Topology” on page 1-12 illustrates the communications between various components as well as the ports on which those communications are received.

The following paragraphs outline these communications. The references to the Vergence Vault are actually to the Virtual IP address or DNS name for Vault system, rather than to a specific vault. For more details on the Virtual IP address please see the *Vergence Context Vault User’s Guide.*

Web Applications on a Windows Desktop

To support Web-based applications, the network configuration must be such that:

- The application can send HTTP messages on port 80 to the Vergence Vaults.
- The client desktops or the Citrix server can be addressed by IP Address from the Vergence Vaults.
- The Vergence Vaults can send HTTP messages on port 2116 to the application (either the client desktop or the Citrix server).
- The Administrator’s Desktop can send LDAP messages on port 389 and HTTPS messages on port 10000 to the Vergence Vaults.
- To perform client desktop specific configuration and monitoring, the Administrator’s desktop can send HTTP messages on port 2116 to the application.
- The Vergence Vaults can send HTTP messages on port 80 to the application Web server.
- The client desktops can send HTTP messages on port 80 to the application Web server.
- The Vergence Vaults can send SMTP messages on port 25 to the Sentillion SMTP server or to a local SMTP server that will relay to Sentillion’s SMTP server.
- If you request support from Sentillion, the support staff will need access to the Vergence Vaults on port 22.
- If a DNS name rather than an IP address is used for the Vergence Vaults, the DNS name can be resolved on the client desktops and the application Web server.
- If a DNS name rather than an IP address is used for the application Web server, the DNS name can be resolved on the client desktops and by the DNS server the Vergence Vaults are configured to use.
- If an SNTP server has been configured, the Vergence Vault can send SNTP messages on port 123 to the configured SNTP server.

COM Applications on a Windows Desktop

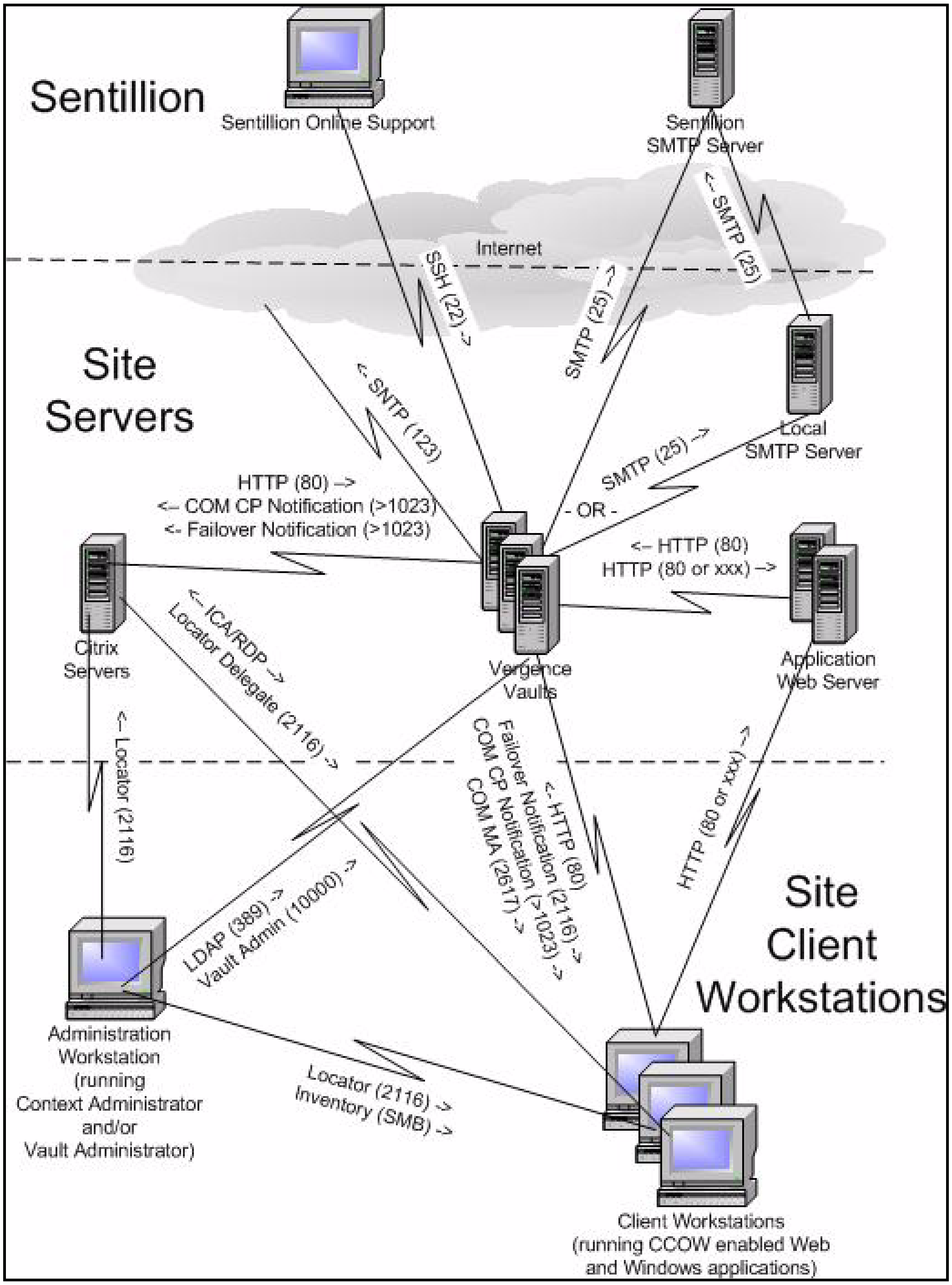
Further, to support CCOW-enabled COM-based applications, the network configuration must be such that:

- The Vergence Vault can send HTTP messages on a dynamically allocated TCP/IP port (>1023) to the client desktop.
- If COM-based Mapping Agents are enabled on the client desktop, the Vergence Vault can send HTTP messages on port 2617 to the client desktops.

COM Applications on a Citrix Server

Furthermore, to support CCOW-enabled COM-based applications running on a Citrix® server, the network configuration must be such that:

- Normal Citrix communication (ICA/RDP) between the Citrix server and the desktop is supported.
- The Citrix Server may send HTTP messages on port 2116 to the client desktop, depending on which mode the Vergence Locator on Citrix is running (delegate or noDelegate). See “Configuring Vergence Locator Properties” on page 3-4.
- The client sessions on the Citrix Server can send HTTP messages on dynamically allocated ports (>1023) to the Citrix client desktops.
- The Vergence Vault can send HTTP messages on a series of dynamically allocated ports (>1023) to the client sessions on the Citrix Server.
- The client sessions on the Citrix Server can send HTTP messages on port 80 to the Vergence Vault.



Vergence Network Topology

TCP/IP Port Usage

The following tables provide details of the communications discussed in the previous section.

Web Applications on a Windows Desktop

These communications are required to support Web applications on a Windows desktop.

Source	Destination	Destination Port	Protocol	Description
Client Desktop	Vergence Vault	80	HTTP	CCOW messages
Client Desktop	Application Web Server	80 (or other, determined by Web application)	HTTP	Browser-based applications
Vergence Vault	Client Desktop	2116	HTTP	Failover notification
Vergence Vault	Application Web Server	80 (or other, determined by Web application)	HTTP	CCOW messages to Web application participants
Vergence Vault	Time Server	123	SNTP	Get time from configured time server

COM Applications on a Windows Desktop

The following table lists additional communications required to support COM applications running on a Windows desktop.

Source Component	Destination Component	Destination Port	Protocol	Description
Vergence Vault	Client Desktop	>1023; dynamically assigned	HTTP	CCOW messages to local COM application participants
Vergence Vault	Client Desktop	2617	HTTP	Requests to COM-based Mapping Agents (optional)

COM Applications

The following additional communications are required.

Source Component	Destination Component	Destination Port	Protocol	Description
Citrix Server	Client Desktop	2116	HTTP	Delegated locate requests to Vergence Locator
Citrix Server	Client Desktop	>1023	HTTP	CCOW listener notification messages to Web listener applets

Vergence Applications

These communications are required to administer the Vergence system.

Source Component	Destination Component	Destination Port	Protocol	Description
Administrator’s Desktop	Vergence Vault	389	LDAP	LDAP database updates (configuration)
Administrator’s Desktop	Vergence Vault	10000	HTTPS	Browser-based Vault configuration
Administrator’s Desktop	Client Desktop	2116	HTTP	Locate request to Vergence Locator
Administrator’s Desktop	Client Desktop	SMB	SMB	Network scan to locate desktops running Desktop Components
Vergence Vault	SMTP Server	25	SMTP	Site statistics e-mail to Sentillion
Sentillion Support	Vergence Vault	22	SSH	Access for Sentillion Support when requested by the site

2

Installing the Software

This chapter describes the process of installing the Vergence Desktop Components.

Step 1: Install

☞ You must uninstall any previous versions of Vergence Desktop Components. If you have previously installed Sentillion’s Vergence Context Manager, or if you have installed a copy of Sentillion’s Vergence Desktop Vault, then you must uninstall these software packages as well.

Desktop Components need to be installed in the locations indicated in the table:

Application Mix	Cixtrix Server	Client Desktop
Remote Desktop	X	
Only published applications	X	
Published applications and locat applications (COM or Web)	X	X
Local applications only		X

If you are installing on a Citrix server, you must not run `setup.exe` directly. (See below.) In addition, please read Chapter 3, “Vergence Products in a Citrix Environment” for configuration information.

1. *If you are installing on a Citrix server:*

   You must install the Desktop Components in a global mode using **Control Panel > Add/Remove Programs > Add New Programs** to run **`setup.exe`**.

   --OR--

   Installing on a desktop:

   When you install the Desktop Components from the CD-ROM, the Desktop Components `setup.exe` program should start automatically. If it does not start, navigate to the top-level directory on the CD and double-click **`setup.exe.`**

2. The **Sentillion Vergence Desktop Components** splash screen displays. Read the Welcome screen information and click **Next**.
3. Read the license agreement and click **Yes** if you agree to the terms.
4. On the **Choose Destination Location** dialog, either click **Browse** to navigate to a new directory or click **Next** to approve the default location for the files. This is the directory into which the Vergence Desktop Components will be installed.
5. *If this installation is on a Citrix server,* then select **Vergence Locator for Citrix**.

☞ The Vergence Locator for Citrix installs the Vergence Locator as a service.

6. Select **Next**. In the **Context Vault Virtual IP Address** dialog, enter the **Virtual IP address** or the DNS name for your system of Vergence Vaults.

☞ The *Virtual IP address* is the IP address or DNS name that represents your system of Context Vaults. The Virtual IP address works in conjunction with Vergence load balancing, as described in “Context Vault Replication, Load Balancing, and Failover” in the *Vergence Context Vault Installation Guide.*

If you use a DNS name for your system of Context Vaults, client desktops must be able to resolve the name.

7. After the software is loaded, click **Next** to view the **Readme** file for last minute information that will help you use the Desktop Components.
8. After you read the Readme file, click **Finish**.
9. To finish a Citrix installation, exit out of the Control Panel.

For desktop installations, a shortcut is created in the **Start** menu that will start the Vergence Locator program whenever the computer starts up.The installation process also launches this program. For Citrix installations, the Locator runs as a service.

Installations Requiring COM-Based Mapping Agents

The CCOW standard enables the implementation of mapping agents either via COM or HTTP. By default, the Sentillion Vergence Desktop Components are configured to work with HTTP-based Mapping Agents. To enable support for local COM-based mapping agents through the Mapping Agent Proxy, see “Enabling COM-Based Mapping Agents” on page 4-3.

Step 2: Verify the Installation

Context Vault Installations

If you have already installed one or more Vergence Context Vaults, you can verify that you have installed the Vergence Desktop Components correctly. See the *Vergence Context Vault User's Guide* for instructions on how to install your Vaults.

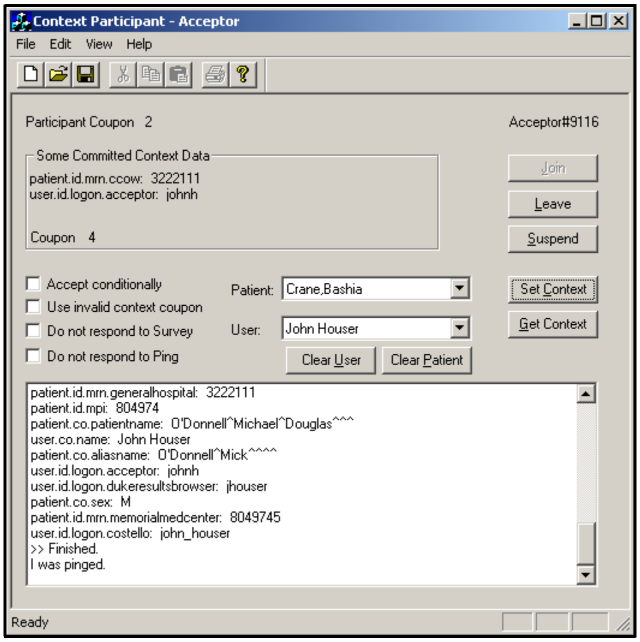
Ensure that the icon for the Vergence Locator program, `VergenceLocator.exe`, displays in your system tray for a clinical desktop installation. Vergence Locator starts automatically during the installation of the Vergence Desktop Components and every time you log onto your computer.

Verify that the installation is complete and operating properly by using the **Acceptor** test program that has been included with the Sentillion software, using the steps below.

Step 2A – Set Up the Acceptor Test Program

The default configuration supports using the Acceptor test program to test Patient Link. Acceptor is a CCOW-compliant, COM-based Windows program. For testing purposes, you should leave all the check boxes in their un-checked state.

You can use Acceptor to verify Patient link and User link. While setting the context, Acceptor's trace window displays messages indicating its progress. The most recent message is at the bottom of the window.



Participant Coupon 2

Acceptor#9116

patient.id.mrn.ccow: 3222111
user.id.logon.acceptor: johnh

Coupon 4

☐ Accept conditionally
☐ Use invalid context coupon
☐ Do not respond to Survey
☐ Do not respond to Ping

Patient: Crane,Bashia

User: John Houser

```
patient.id.mrn.generalhospital:  3222111
patient.id.mpi:  804974
patient.co.patientname:  O'Donnell^Michael^Douglas^^^
user.co.name:  John Houser
patient.co.aliasname:  O'Donnell^Mick^^^^
user.id.logon.acceptor:  johnh
user.id.logon.dukeresultsbrowser:  jhouser
patient.co.sex:  M
patient.id.mrn.memorialmedcenter:  8049745
user.id.logon.costello:  john_houser
>> Finished.
I was pinged.
```

To use Acceptor to test User Link, perform these steps.

1. Request the Acceptor passcode for your site from your Sentillion Client Services representative.
2. Use the **Context Administrator** to add Acceptor as a trusted application. For details, see *Vergence Context Administrator's User Guide*.

Step 2B – Start the Acceptor Test Program

Run the Acceptor test program. If you installed Desktop Components in the default directory, the path to the program is:

```
C:\Program Files\Sentillion\DesktopComponents\Acceptor.exe
```

☞ Do *not* check any of the check boxes on Acceptor.

Step 2C – Join the Common Context

1. To join the common context, click the **Join** button and observe the messages that are displayed.

☞ If you didn’t use Context Administrator to add Acceptor as a trusted application (see Step 2A on the previous page), you might see a dialog indicating a failure to initialize binding. This is normal.

2. Click **OK** to continue.

Step 2D – Set the Context

To instruct Acceptor to set the context:

1. Choose a patient from the list of patients provided in the **Patient** selection list. Click **Join**.
2. Choose a user from the list of users provided in the section labeled **User**.
3. Click the **Set Context** button.

☞ If you didn’t use Context Administrator to add Acceptor as a trusted application (see Step 2A on the previous page), Acceptor is not configured to set the secure user subject. You will only be able to set the patient subject.

Step 2E -Leave the Context and Exit

Instruct Acceptor to leave the common context by doing the following:

1. Clicking the **Leave** button.
2. Choosing **File** > **Exit**.

☞ After testing, you must remove Acceptor as a trusted application. Leaving Acceptor configured on a live system could create a security risk, since it is a widely available test program with a well known passcode. See the *Context Administrator User's Guide* for details.

Congratulations!

The Desktop Components software has been properly installed and is ready for you to use.

3

Vergence Products in a Citrix Environment

This chapter describes the support provided for the Citrix environment. A Citrix-specific version of Vergence Locator is installed on the Citrix server that allows you to configure whether and how Locator operates on the client desktops.

You only need to install the Vergence Desktop Components on the client machines only if there is a need to share context with applications that are installed and running locally or through a browser running on the client.

You need to install on a Citrix server if you want to run Vergence products in a Citrix environment.

For remote published applications:

- All CCOW-enabled published applications must be served from the same Citrix server for the same client computer. We do not support sharing context among CCOW enabled application that are being served from different Citrix servers for the same client machine unless you are running a single Context Vault system.

For remote desktops:

- Each remote desktop session will have its own context session. Context will be shared with applications running in other remote desktop sessions, only if the remote delegateType is set to noDelegate. See the descriptions of Delegate, noDelegate, and DelegateContinue, under “Modes of Operation” on page 3-3.

- Citrix remote Desktop sessions with CCOW applications cannot be disconnected and then resumed on a different client. We recommend that Citrix be configured so that disconnected sessions are logged off to reset a broken or timed-out connection. See “Configuring Citrix ICA to Reset on Disconnections” on page 3-7.

- We do not support hosting a Citrix published application from within a Citrix remote desktop session.

Modes of Operation

The Vergence Desktop Components on Citrix may delegate the CCOW Context Management Registry Locate call so that applications running in a Citrix session will share context with applications running on the local desktop.

The operating system launches only one Vergence Locator process during startup. The single Vergence Locator process handles the Context Management Registry requests from all user sessions on that Citrix Server. The Context Management Registry requests may be delegated from the Citrix Server’s Vergence Locator to the Vergence Locator running on the local desktop from which the Citrix client session is started. The descriptions below and the diagram that follows describes the modes in detail.

You can configure the Locator in the following ways:

- **delegate** -- Use this setting when there is a mix of applications running through Citrix and on the local desktop. This setting allows all applications run by one users on the desktop or on a Citrix server to share context. The Citrix server must be able to connect to a local desktop; you cannot use Delegate if there are firewalls between the desktop and the Citrix server.

- **noDelegate** -- Use this setting when there are no desktops that need to share context with applications running locally and on a Citrix server. Published applications will share common context as long as all published applications are being hosted on the same Citrix server for that desktop or you are running a single Context Vault system. Remote desktops only share context among applications running within a remote desktop session. An application on a client desktop will not share the same context as Citrix applications. The Citrix server must be able to connect to a local desktop; you cannot use this setting if there are firewalls between the desktop and the Citrix server.

- **delegateContinue** -- Use this setting if you want applications to share context between Citrix and local applications. If the Locator running on the Citrix server cannot delegate, it will revert to running in the No Delegate mode for that context session.

Citrix-Specific Configuration

If you are using a Citrix server, you must meet these additional requirements.

Installation

Vergence Desktop Components must be installed from the Windows Control Panel, using **Add/Remove** programs. This installs the Vergence Desktop Components in the global mode in Citrix. Please see “Step 1: Install” on page 2-2.

Check the Citrix installation option when prompted during the Vergence Desktop Component installation procedure from the installation CD-ROM.

Vergence Locator Service

The Vergence Locator runs as a service that starts at system reboot and stops at system shutdown. If you want to manually stop or start the Vergence Locator Service, use the Service applet from the Windows Control Panel.

Configuring Vergence Locator Properties

You must configure a VergenceLocatorCommon.properties file for each Citrix server. The VergenceLocatorCommon.properties files allows you to configure the Locator for your Citrix environment.

☞ All names and values are case sensitive.

The VergenceLocatorCommon.properties file contains the following information:

```
#Mon Jun 24 17:42:51 EDT 2002
manufacturer=Sentillion, Inc.
targetOSRev=95(OSR2), 98, NT(SP3), W2K
targetOS=Windows
maProxyName=W2CMA
revMajorNumber=3.3
terminalService=true
delegateType=noDelegate
delegateTimeout=5000
whenInstalled=unavailable
desktopIdType=clientName
maProxyPort=$port$
noDialog=false
partNumber=0400-1032
revMinorNumber=5.8719
orgId=01028
```

Of these parameters you need to configure the following, as described in the tables below.

- `delegateType`
- `desktopIdType`

Use the values described in this table for `delegateType`.

Value	Description

`noDelegate`
`(default)`
	Use this setting when there is a mix of applications running through Citrix and on the local desktop. This setting allows all applications run by one users on the desktop or on a Citrix server to share context. The Citrix server must be able to connect to a local desktop; you cannot use Delegate if there are firewalls between the desktop and the Citrix server.

Value	Description
`delegate`	Use this setting when there are no desktops that need to share context with applications running locally and on a Citrix server. Published applications will share common context as long as all published applications are being hosted on the same Citrix server for that desktop or you are running a single Context Vault system. Remote desktops only share context among applications running within a remote desktop session. An application on a client desktop will not share the same context as Citrix applications. The Citrix server must be able to connect to a local desktop; you cannot use this setting if there are firewalls between the desktop and the Citrix server.
`delegateContinue`	Use this setting if you want applications to share context between Citrix and local applications. If the Locator running on the Citrix server cannot delegate, it will revert to running in the No Delegate mode for that context session.

Use the table below to determine the values for `desktopIdType`. In order to obtain logs and status information using the Context Administrator, the CA must be configured with the names or IP addresses of all the Citrix servers.

Value	Description

`clientName`
`(default)`
	Use Citrix connection name to identify sessions. Citrix defaults this value to the computer's host name. You must ensure that all Citrix `clientNames` are unique.

Value	Description
`clientIP`	Only use this setting if the client machines have static unique IP addresses and are not using DHCP.

Configuring Citrix ICA to Reset on Disconnections

Disconnected Citrix sessions are not supported, so you must configure Citrix to terminate connections when those connections become disconnected. Lingering disconnected sessions could cause a potential security vulnerability as users might be able to access lingering prior context sessions. By terminating all disconnected sessions, this security vulnerability is eliminated.

There are two parts to this process. First, the Citrix server must be configured so that all disconnections are properly detected. Second, the Citrix server must be configured to terminate all sessions when they have been disconnected.

Detecting All Disconnections

In some cases (client power failure, etc.) the Citrix server might not detect that the session has been disconnected and the session will still appear to be active, even though the client has lost its connection. By default, Citrix does not detect this correctly. (See the Knowledge Base article CTX708444 at www.citrix.com for more information.) The default Registry settings must be modified to fix this behavior.

Key	Value

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`	`IcaEnableKeepAlive`
	`REG_DWORD: 1`

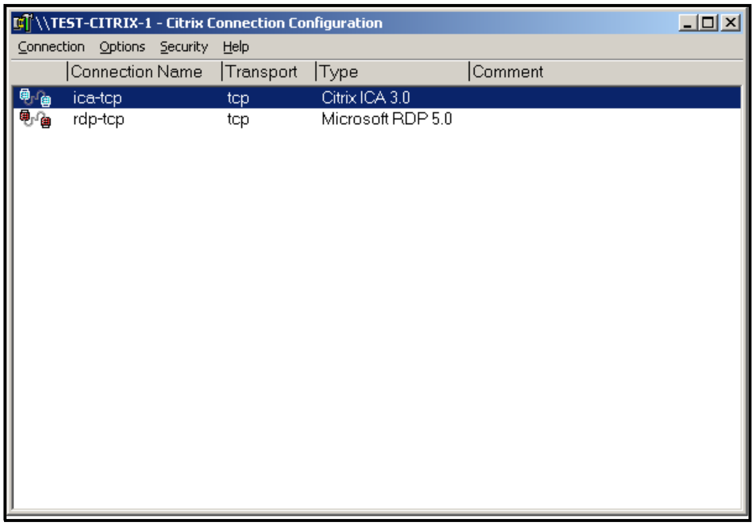
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix`	`ICAKeepAliveInterval`
	`REG_DWORD: 30`

By setting `ICAKeepAliveInterval`, the Citrix server will send a watchdog packet to the Citrix client on a configurable interval. Setting the `ICAKeepAliveInterval` to 30 will cause this watchdog packet to be sent once every minute. There are other Windows TCP/IP parameters that may need to be set in the Registry, depending on your environment. Please refer to Knowledge Base article CTX708444 at www.citrix.com for more information.

Configuring the Citrix Server to Terminate Disconnected Sessions

After you set the Registry Keys, use the Citrix Connection Configuration Program to handle the disconnect.

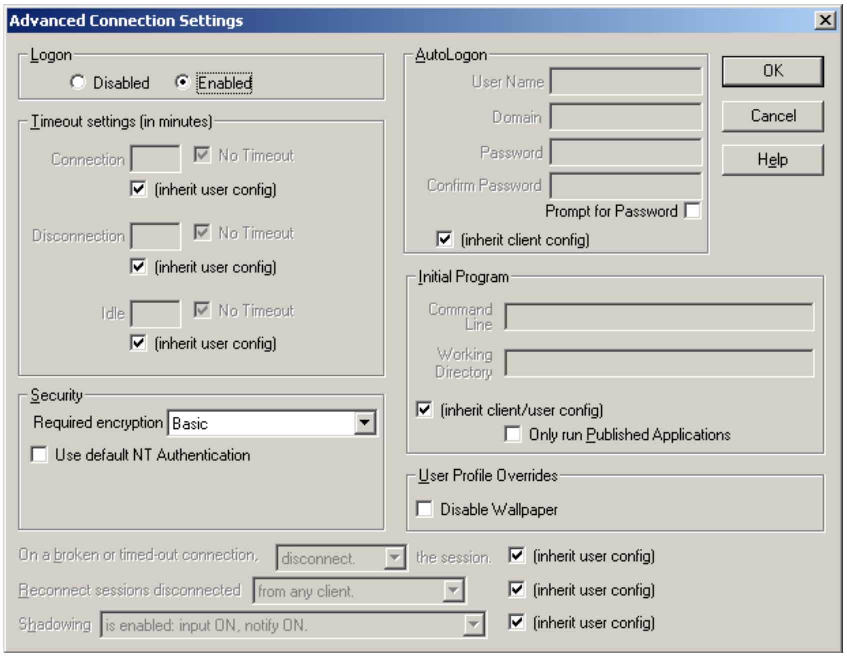
1. From **Programs -> Citrix -> MetaFrame XP**, click on **Citrix Connection Configuration**.



Connection Name	Transport	Type	Comment
ica-tcp	tcp	Citrix ICA 3.0	
rdp-tcp	tcp	Microsoft RDP 5.0	

]

2. Right click on **ica-tcp** and select **Edit**. The Advanced Connection Settings dialog box displays.



Advanced Connection Settings

Logon
○ Disabled ● Enabled

Timeout settings (in minutes)
Connection ☑ No Timeout
☑ (inherit user config)
Disconnection ☑ No Timeout
☑ (inherit user config)
Idle ☑ No Timeout
☑ (inherit user config)

Security
Required encryption: Basic
☐ Use default NT Authentication

AutoLogon
User Name
Domain
Password
Confirm Password
Prompt for Password ☐
☑ (inherit client config)

Initial Program
Command Line
Working Directory
☑ (inherit client/user config)
☐ Only run Published Applications

User Profile Overrides
☐ Disable Wallpaper

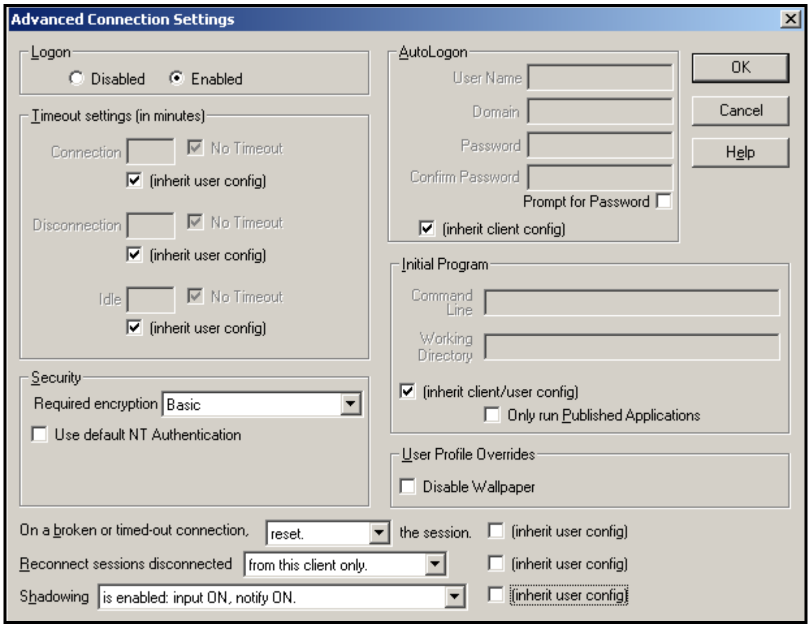
On a broken or timed-out connection, disconnect the session. ☑ (inherit user config)
Reconnect sessions disconnected from any client. ☑ (inherit user config)
Shadowing is enabled: input ON, notify ON. ☑ (inherit user config)

3. In the lower portion of the dialog box, uncheck each of the last three items one at a time and change them as follows:

   - Change **On a broken or timed-out connection** to **reset**.
   - Change **Reconnect sessions disconnected** to **from this client only**.

- Change **Shadowing** to **is enabled: input ON, notify ON**.

The dialog box will look like the following when you are done:



Advanced Connection Settings

Logon
○ Disabled ● Enabled

Timeout settings (in minutes)
Connection ☑ No Timeout
☑ (inherit user config)
Disconnection ☑ No Timeout
☑ (inherit user config)
Idle ☑ No Timeout
☑ (inherit user config)

Security
Required encryption: Basic
☐ Use default NT Authentication

AutoLogon
User Name
Domain
Password
Confirm Password
Prompt for Password ☐
☑ (inherit client config)

Initial Program
Command Line
Working Directory
☑ (inherit client/user config)
☐ Only run Published Applications

User Profile Overrides
☐ Disable Wallpaper

On a broken or timed-out connection, reset. the session. ☐ (inherit user config)
Reconnect sessions disconnected from this client only. ☐ (inherit user config)
Shadowing is enabled: input ON, notify ON. ☐ (inherit user config)

Server Security

After installation, protect the Desktop Component files as you would any other application files running in a server environment. Protect all the Desktop Component files by making them Read Only to individual users, so that users cannot delete or change them. Please see “Files Copied During Installation” on page 5-3 for more information.

Logging

By default, the Vergence Locator Service does not perform logging. If required by Sentillion support for debugging, turn on logging by adding the service startup parameter **-l** (lowercase “L,” for “logging”) to the Locator Service.

Deploying the Configured Vergence Locator

After you configure the Locator, follow these steps to have it be available to your client workstations.

1. Select **Restart**.
2. Select **Control Panel**.
3. Select **Admin Tools**.
4. Select **Services**.
5. Select **Stop, Start**.

4

Operating Tips

This chapter describes things you might find useful to know once you have installed the Vergence Desktops Components.

In a normal production environment the Vergence Desktop Components require no administrative actions or intervention. The following sections provide information that may be useful in resolving exceptional conditions.

Context Manager Proxy

The Context Manager Proxy for COM applications is implemented by `c2w_cm.exe` and `c2w_cm.dll`. The Context Manager Proxy launches automatically when the first CCOW-compliant COM-based application connects to it and terminates automatically when the last CCOW-compliant COM-based application disconnects. These components reside at:

```
<Vergence Installation path>\DesktopComponents\COMAdapters
```

Generally, only one `c2w_cm.exe` process executes at a time when Desktop Components reside on the desktop. However, sometimes you may notice more than one for a short period of time. This is normal as a `c2w_cm.exe` may take several minutes before it completely terminates. Only one of the `c2w_cm.exe` processes is the active `c2w_cm.exe` for the desktop.

If at any time `c2w_cm.exe` is unable to start up, an error is logged in the `<Vergence Installation path>\DesktopComponents\COMAdapters\log\StartUpErrors.txt` file. Each time there is a start up error, the file is overwritten with the most recent information.

If you only want to run Web applications, not COM applications, you can remove support for COM applications by unregistering the Context Manager Proxy `c2w_cm` server. Please contact Sentillion Customer Support if you require help with this process.

Enabling COM-Based Mapping Agents

Vault Configuration

You must use the Vault Administrator to configure each of your Vaults to use the COM-based mapping agents. See the document *Vergence Context Vault User's Guide* for details.

Desktop Configuration

1. Make sure your COM Patient or User Mapping Agent is registered in the Windows Registry.
2. The Vergence Locator serves as the COM Mapping Agent bridge and must be configured to look for COM Mapping Agents. Once you turn on support for COM-based mapping agents, you will use default port of 2617.
   - To configure the desktop for COM Mapping Agents for the current login session only, terminate the `VergenceLocator.exe` program and manually re-launch it with the **-m** and **-p** command line switches followed by the desired port number.

     ```
     "C:\Program Files\Sentillion\DesktopComponents\VergenceLocator.exe" -m -p 2211
     ```

   - To configure the desktop on a permanent basis, see "Changing the Port Number for COM Mapping Agents," below.

Changing a Port Number for COM Mapping Agents

1. Click **Start > Programs > Startup** then right click on **Vergence Locator.**
2. Select **Properties** and select the **Shortcut** tab.
3. In the **Target** text box, change the port number by typing **-m -p <number>** at the end of the path for the Vergence Locator. For example:

   ```
   "C:\Program Files\Sentillion\DesktopComponents\VergenceLocator.exe" -m -p 2211.
   ```

Vergence Locator Functionality

When you install the Desktop Components, you will see an icon for the Vergence Locator in the system tray of a non-Citrix desktop. The behavior of the icon indicates the following:

- When the icon animates, it indicates that the Locator has received a request and is processing it.
- When the icon contains a red dot in the center, a communication to the Vault failed.

Moving the mouse over the icon displays the Locator version number.

5

System Changes

This chapter describes the files that are copied onto your computer when you install the Vergence Desktop Components. The changes to the Windows Registry settings are also described.

You don’t need this information to install or use the Vergence Desktop Components; it is provided for completeness.

Directories Created During Installation

The following table lists the subdirectories created in the installation directory (by default, `C:\Program Files\Sentillion\DesktopComponents`).

Directory name	Comments
`\DesktopComponents`	Contains the executable files, icon files, dynamic link libraries, etc., that comprise the Vergence Desktop Components software.
`\DesktopComponents \COMAdapters`	Contains the subset of executable files, dynamic link libraries, and type libraries for communication between CCOW-compliant COM-based applications and Vergence Vaults.
`\DesktopComponents \COMAdapters\Log`	Contains the Context Manager Proxy’s log files.
`DesktopComponents\Data`	Contains configuration files for the Vergence Locator.
`\DesktopComponents\log`	Contains the Vergence Locator log file.

Files Copied During Installation

The following tables list the files copied to subdirectories created in the installation directory (by default, `C:\Program Files\Sentillion\DesktopComponents`).

Files Copied to \DesktopComponents

File name	Comments
`Acceptor.exe`	Acceptor test program executable.
`ContextData.vdk`	Data file used by Acceptor test program.
`CryptoKeyTool.exe`	Executable that cleans the cryptographic key container resources from the operating system.
`CryptoWrapper.dll`	Cryptographic wrapper dynamic link library used by the Acceptor executable to encapsulate cryptographic operations performed by client applications.
`DesktopInstallGuide.pdf`	This document in PDF format.
`Disclaimer.txt`	Disclaimer text file.
`Readme.htm`	Document containing last-minute product information.
`Uninst.isu`	File used to uninstall the Desktop Components.
`UnInstMgr.dll`	File used to uninstall the Desktop Components.
VergenceContextor.dll	Contextor dynamic link library.
`VergenceLocator.exe`	Executable that runs the Vergence Locator program.
`VergenceLocatorService.exe`	For Citrix installations only, an executable needed to run `VergenceLocator.exe` as an NT service.

Files Copied to \DesktopComponents\COMAdapters

File name	Comments
`c2w_cm.dll`	`c2w_cm.exe` uses this dll file. It translates COM messages to HTTP messages to send to and from the Context Manager.
`c2w_cm.exe`	Context Manager Proxy. This acts as a proxy for COM applications.
`C2WCNX.dll`	The Context Manager Proxy specialized for Citrix environments.
`ContextManager.tlb`	Context Manager type library used for COM applications.

Files Copied to \DesktopComponents\Data

File name	Comments
`ContextVault.dat`	Contains the Virtual IP address for your system of replicated Context Vaults.

Files Created in \DesktopComponents\Data

File name	Comments
`desktopId.txt`	Text file created by `VergenceLocator.exe` to store this desktop’s unique Vergence identifier.

Files Created in \DesktopComponents\ComAdapters\Log

File name	Comments
`Startuperrors.txt`	Start-up error log for the Context Manager Proxy. Each time a startup error occurs, this file is overwritten with the latest error. See “Context Manager Proxy” on page 4-2 for more information.

Files Created in \DesktopComponents\Log

File name	Comments
`VergenceLocator.log`	Run log for the Vergence Locator. Contains both information and errors. If you are running in a Citrix environment, also see “Vergence Locator Service” on page 3-4 and “Logging” on page 3-10.

File Available on the Media

File name	Comments
`rp505enu.exe`	The Adobe Acrobat Reader 5.0 file required for viewing the online version of this document.

Registry Keys Set

The following tables list the Windows Registry keys (including name:type:value) that are set on your computer during installation of the Vergence Desktop Components.

HKEY_LOCAL_MACHINE/SOFTWARE Settings

Key	Name: Type: Value
/Sentillion/COMAdapters	<Path>: REG_EXPAND_SZ: *installation path*
/Sentillion/DesktopComponents	<InstalledVersion>: REG_SZ: *num.num.num.num* (e.g., 3.2.96.0)
	<Path>:REG_EXPAND_SZ: *installation path*
	Type: REG_SZ: Citrix
/Sentillion/DesktopComponents/3.3	*empty*

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services Settings

These keys are only used for Citrix installations.

Key	Name: Type: Value
/VergenceLocatorService	<DisplayName>: REG_SZ: VergenceLocatorService
	<Error Control>: REG_DWORD: 1
	<ImagePath>: REG_EXPAND_SZ: *Installation Path*
	<ObjectName>: REG_SZ: LocalSystem
	<Start>: REG_DWORD: 2
	<Type>: REG_DWORD: 16
	Description REG_SZ: “Locates Vergence Context Manager in a Citrix Environment”

HKEY_CLASSES_ROOT Settings

This table is an alias for HKEY_LOCAL_MACHINE/SOFTWARE/CLASSES.

Key	Name: Type: Value
/AppID/{0DDBCE29-C69A-11D2-BE3D-080009D14A99}	<No Name>: REG_SZ: ContextManager
/CCOW.ContextManager	<No Name>: REG_SZ: ContextManager Class
/ContextManager.exe	<No Name> : : REG_SZ: <No value>
	AppID: REG_SZ: {0DDBCE29-C69A-11D2-08009D14A99}
/CCOW.ContextManager/CLSID	<No Name>: REG_SZ: {0DDBCE35-C69A-11D2-BE3D-080009D14A99}
/CCOW.ContextManager.1	<No Name>: REG_SZ: ContextManager Class
/CCOW.ContextManager.1/CLSID	<No Name>: REG_SZ: {0DDBCE35-C69A-11D2-BE3D-080009D14A99}
/CLSID/{0DDBCE35-C69A-11D2-BE3D-080009D14A99}	<No Name>: REG_SZ: ContextManager Class
	AppID: REG_SZ: {0DDBCE29-C69A-11D2-BE3D-080009D14A99}
/CLSID/{0DDBCE35-C69A-11D2-BE3D-080009D14A99}/LocalServer32	<No Name>: REG_SZ: *path to c2w_cm.exe*
/CLSID/{0DDBCE35-C69A-11D2-BE3D-080009D14A99}/ProgID	<No Name>: REG_SZ: CCOW.ContextManager.1
/CLSID/{0DDBCE35-C69A-11D2-BE3D-080009D14A99}/VersionIndependentProgID	<No Name>: REG_SZ: CCOW.ContextManager

Registry Keys Set

Key	Name: Type: Value
/CLSID/{19E7D790-D020-11D2-BE3E-080009D14A99}	<No Name>: REG_SZ: Sentillion.ContextManager
/CLSID/{19E7D790-D020-11D2-BE3E-080009D14A99}/ImplementedCategories/{BE0975F0-BBDD-11CF-97DF-00AA001F73C1}	*empty*
/CLSID/{19E7D790-D020-11D2-BE3E-080009D14A99}/InProcServer32	<No Name>: REG_SZ: *path to c2w_cm.dll or C2WCMX.dll*
	<JavaClass>: REG:SZ: com/sentillion/contextmanagerproxy/cmactivex/CMActiveXProxy
	<ThreadingModel>: REG_SZ: Both
/CLSID/{19E7D790-D020-11D2-BE3E-080009D14A99}/ProgID	<No Name>: REG_SZ: Sentillion.ContextManager
/CLSID/{19E7D790-D020-11D2-BE3E-080009D14A99}/TypeLib	<No Name>: REG_SZ: {0C6138B0-D020-11D2-BE3E-080009D14A99}
/CLSID/{19E7D790-D020-11D2-BE3E-080009D14A99}/Version	<No Name>: REG_SZ: 1.0
/Sentillion.ContextManager	<No Name>: REG_SZ: Sentillion.ContextManager
/Sentillion.ContextManager/CLSID	<No Name>: REG_SZ: {19E7D790-D020-11D2-BE3E-080009D14A99}
/Sentillion.ContextParticipantProxy	<No Name>: REG_SZ: ContextParticipantProxy Class
/Sentillion.ContextParticipantProxy/CLSID	<No Name>: REG_SZ: {A918F0E0-DF21-11D2-BE3E-080009D14A99}

Key	Name: Type: Value
/Sentillion.ContextParticipantProxy/CurVer	<No Name>: REG_SZ: Sentillion. ContextParticipantProxy.1
/Sentillion.ContextParticipantProxy.1	<No Name>: REG_SZ: ContextParticipantProxy Class
/Sentillion.ContextParticipantProxy.1/CLSID	<No Name>: REG_SZ: {A918F0E0-DF21-11D2-BE3E-080009D14A99}
/Sentillion.CryptoWrapper	<No Name>: REG_SZ: CCOWCryptoWrapper Class
/Sentillion.CryptoWrapper/CurVer	<No Name>: REG_SZ: Sentillion.CCOWCryptoWrapper.Sentillion.CryptoWrapper.1
/Sentillion.CryptoWrapper.1	<No Name>: REG_SZ: CCOWCryptoWrapper Class
/Sentillion.CryptoWrapper/CLSID	<No Name>: REG_SZ: {7F6A0460-A664-11D2-8080C766F3D8}
/TypeLib/{0DDBCE28-C69A-11D2BE3D-080009D14A99}/1.0/0	*empty*
/TypeLib/{0DDBCE28-C69A-11D2BE3D-080009D14A99}/1.0/0/Win32	<No Name>: REG_SZ: *path to c2w_cm.dll or C2WCMX.dll*
TypeLib/{0DDBCE28-C69A-11D2BE3D-080009D14A99}/1.0/Flags	<No Name>:REG_SZ:0
/TypeLibTypeLib/{0DDBCE28-C69A-11D2BE3D-080009D14A99}/1.0/HELPDIR	<No Name>: REG_SZ: *installation path to ComAdapters*

Registry Keys Set

Index