SINGLE SIGN-ON/USER CONTEXT (SSO/UC)

INSTALLATION GUIDE

Kernel Patch XU*8.0*337

September 2006

Department of Veterans Affairs
VistA Health Systems Design & Development (HSD&D)
Infrastructure & Security Services (ISS)

Revision History

Documentation Revisions

The following table displays the revision history for this manual. Revisions to the documentation are based on patches and new versions released to the field.

Date	Revision	Description	Author(s)
09/27/06	1.0	Initial SSO/UC software and documentation release. **Kernel Patch XU*8.0*337**	ISS SSO/UC Development Team Oakland, CA and Bay Pines, FL OIFO: • Project Manager—Dan Soraoka • Project Planner—Laura Rowland • Developers—Alan Chan, Kyle Clarke, Wally Fort, Jose Garcia, Joel Ivey, and John Vrooland • SQA—Matt Alderman • Technical Writer—Thom Blom

Table i. Documentation revision history

Patch Revisions

For a complete list of patches related to this software, please refer to the Patch Module on FORUM.

NOTE: Kernel (i.e., Kernel Patch XU*8.0*337) is the designated custodial software package for SSO/UC. However, SSO/UC comprises multiple patches and software releases from several VistA/Health*e*Vet-VistA applications.

REF: For the specific VistA M Server software patches required for the implementation of SSO/UC, please refer to Table 1-2 in Chapter 1, "Pre-Installation Instructions" in this manual.

Contents

Figures and Tables

Acknowledgements

The Single Sign-On/User Context (SSO/UC) Project Team consists of the following Development and Infrastructure Services (DaIS) and Infrastructure & Security Services (ISS) personnel (listed alphabetically within each category/title):

- ISS Program Manager—Larry Weldon
- ISS Project Manager—Dan Soraoka
- Centralized Planner Support Team (CPST)—Laura Rowland
- Developers—Alan Chan (KAAJEE), Kyle Clarke (VistALink), Wally Fort (Kernel), Jose Garcia (KAAJEE), Joel Ivey (RPC Broker), and John Vrooland (FatKAAT)
- Functional Analysts—Lauren Gorgoglione
- Software Quality Assurance (SQA)—Matt Alderman
- Technical Writer—Thom Blom

The SSO/UC Project Team would like to thank the following sites/organizations/personnel for their consultation and assistance in reviewing and/or testing SSO/UC-related software and documentation (listed alphabetically):

- Care Management (CM)/Health*e*Vet Development Team
- CCOW Team—Charles Arceneaux, Patrick (Tim) Landy, Dwyla Mosher, and David Tuma
- Computerized Patient Record System (CPRS) GUI Development Team
- Sentillion, Inc.—David Fusari, Karl Schoppe, and Eric Weaver
- Vitals Development Team

Orientation

How to Use this Manual

Throughout this manual, advice and instructions are offered regarding the installation and use of SSO/UC and the functionality it provides for Veterans Health Information Systems and Technology Architecture (VistA) and Health*e*Vet-VistA software products.

There are no special legal requirements involved in the use of SSO/UC.

This manual uses several methods to highlight different aspects of the material:

- Various symbols/terms are used throughout the documentation to alert the reader to special information. The following table gives a description of each of these symbols/terms:

Symbol	Description
ℹ	**NOTE/REF:** Used to inform the reader of general information including references to additional reading material.
⚠	**CAUTION or DISCLAIMER:** Used to inform the reader to take special notice of critical information.
★	**UPGRADES/VIRGIN INSTALLATION:** Used to denote Upgrade or Virgin installation instructions only.

Table ii. Documentation symbol/term descriptions

- Descriptive text is presented in a proportional font (as represented by this font).
- "Snapshots" of computer online displays (i.e., roll-and-scroll screen captures/dialogues) and computer source code, if any, are shown in a *non*-proportional font and enclosed within a box.
  - User's responses to online prompts and some software code reserved/key words will be boldface.
  - References to "**<Enter>**" within these snapshots indicate that the user should press the **Enter** key on the keyboard. Other special keys are represented within < > angle brackets. For example, pressing the **PF1** key can be represented as pressing **<PF1>**.
  - Author's comments, if any, are displayed in italics or as "callout" boxes.

ℹ **NOTE:** Callout boxes refer to labels or descriptions usually enclosed within a box, which point to specific areas of a displayed image.

- Java software code, variables, and file/folder names can be written in lower or mixed case.
- All uppercase is reserved for the representation of M code, variable names, or the formal name of options, field and file names, and security keys (e.g., the XUPROGMODE key).

How to Obtain Technical Information Online

Exported VistA M Server-based file, routine, and global documentation can be generated through the use of Kernel, MailMan, and VA FileMan utilities.

NOTE: Methods of obtaining specific technical information online will be indicated where applicable under the appropriate topic.

Help at Prompts

VistA M Server-based software provides online help and commonly used system default prompts. Users are encouraged to enter question marks at any response prompt. At the end of the help display, you are immediately returned to the point from which you started. This is an easy way to learn about any aspect of VistA M Server-based software.

Obtaining Data Dictionary Listings

Technical information about VistA M Server-based files and the fields in files is stored in data dictionaries (DD). You can use the List File Attributes option on the Data Dictionary Utilities submenu in VA FileMan to print formatted data dictionaries.

REF: For details about obtaining data dictionaries and about the formats available, please refer to the "List File Attributes" chapter in the "File Management" section of the *VA FileMan Advanced User Manual*.

Assumptions About the Reader

This manual is written with the assumption that the reader is familiar with the following:

- VistA/Health*e*Vet-VistA computing environment:
  - Kernel—VistA M Server software
  - Remote Procedure Call (RPC) Broker—VistA M Server software
  - VA FileMan data structures and terminology—VistA M Server software
  - VistALink—VistA M Server and client workstation software
- Microsoft Windows environment
- M programming language
- Object Pascal programming language—RPC Broker
- Java Programming language—VistALink
- CCOW—Sentillion Vergence Context Vault

This manual provides an overall explanation of installing and configuring SSO/UC on the VistA M Server and client/server workstation. It also provides information on the overall functionality provided by SSO/UC. However, no attempt is made to explain how the overall VistA and Health*e*Vet-VistA programming system is integrated and maintained. Such methods and procedures are documented elsewhere. We suggest you look at the various VA home pages on the World Wide Web (WWW) and VA Intranet for a general orientation to VistA and Health*e*Vet-VistA. For example, go to the Veterans Health Administration (VHA) Office of Information (OI) Health Systems Design & Development (HSD&D) Home Page at the following Intranet Web address:

http://vista.med.va.gov/

Reference Materials

Readers who wish to learn more about the SSO/UC-related software should consult the following:

- *Single Sign-On/User Context (SSO/UC) Installation Guide (Kernel Patch XU*8.0*337)*, this manual
- *Single Sign-On/User Context (SSO/UC) Deployment Guide (Kernel Patch XU*8.0*337)*
- SSO/UC Web site: http://vaww.vista.med.va.gov/kernel/sso/index.asp
- *Kernel Systems Manual (Version 8.0)*
- *RPC Broker Installation Guide (XWB*1.1*40)*
- *RPC Broker Developer's Guide (online help, XWB*1.1*40)*
- *RPC Broker Getting Started with the RPC Broker Development Kit (BDK, XWB*1.1*40)*
- *RPC Broker Systems Manual (XWB*1.1*40)*
- *VistALink Installation Guide (Version 1.5)*
- *VistALink Developer/System Manager Manual (Version 1.5)*
- *VistALink Systems Management Guide and Package Security Guide (Version 1.5)*

REF: For more information on VistALink, please refer to the Application Modernization Foundations Web site located at the following Web address:

http://vaww.vista.med.va.gov/migration/foundations/vl/index.htm

- *Sentillion Vergence User Link Installation Instructions*
- *Sentillion Vergence Context Vault User's Guide (Version 3.3)*
- *Sentillion Vergence Desktop Components Installation Guide (Version 3.3)*

VistA/Health*e*Vet-VistA documentation is made available online in Microsoft Word format and Adobe Acrobat Portable Document Format (PDF). The PDF documents *must* be read using the Adobe Acrobat Reader (i.e., ACROREAD.EXE), which is freely distributed by Adobe Systems Incorporated at the following Web address:

http://www.adobe.com/

REF: For more information on the use of the Adobe Acrobat Reader, please refer to the Adobe Acrobat Quick Guide at the following Web address:

http://vista.med.va.gov/iss/acrobat/index.asp

VistA/Health*e*Vet-VistA documentation can be downloaded from the Health Systems Design and Development (HSD&D) VistA Documentation Library (VDL) Web site:

http://www.va.gov/vdl/

VistA/Health*e*Vet-VistA documentation and software can also be downloaded from the Enterprise VistA Support (EVS) anonymous directories:

Albany OIFO	ftp://ftp.fo-albany.med.va.gov/
Hines OIFO	ftp://ftp.fo-hines.med.va.gov/
Salt Lake City OIFO	ftp://ftp.fo-slc.med.va.gov/
Preferred Method	download.vista.med.va.gov

This method transmits the files from the first available FTP server.

DISCLAIMER: The appearance of any external hyperlink references in this manual does not constitute endorsement by the Department of Veterans Affairs (VA) of this Web site or the information, products, or services contained therein. The VA does not exercise any editorial control over the information you may find at these locations. Such links are provided and are consistent with the stated purpose of this VA Intranet Service.

1. Pre-Installation Instructions

Purpose

The purpose of this guide is to provide instructions for installing the Health*e*Vet-Veterans Health Information Systems and Technology Architecture (VistA) Single Sign-On/User Context (SSO/UC) and related software.

SSO/UC is *not* an application but a framework. Users of the software need to understand how it integrates in their working environment. Thus, installing SSO/UC means to understand what jars and files need to be put where and what are the configuration files that you need to have and edit.

SSO/UC provides a secure signon architecture for Vista client/server-based applications. For example:

- Care Management
- Computerized Patient Record System-Rehosted (CPRS)
- Vitals

These VistA client/server-based applications are able to authenticating against Kernel on the VistA M Server via an application graphical user interface (GUI) on the client workstation.

Installation Procedures—Outline

The installation instructions for SSO/UC are organized and described in this guide as follows:

I. Pre-Installation Instructions.

II. VistA M Server Installation Instructions:

    A. Install Kernel Patches

    B. Install RPC Broker Patches

    C. Install VistALink Patches

II. Client workstation Installation Instructions:

    A. Install CCOW Context Monitor

NOTE: Kernel (i.e., Kernel Patch XU*8.0*337) is the designated custodial software package for SSO/UC-related software. However, SSO/UC comprises multiple patches and software releases from several VistA/Health*e*Vet-VistA applications.

REF: For the specific VistA M Server software patches required for the implementation of SSO/UC, please refer to Table 1-2 in this chapter.

NOTE: This manual assumes that the Sentillion Vergence Context Vault V. 3.3 (or higher), which is required for CCOW functionality, is already installed and running on the appropriate server.

Distribution Files

Confirm the following SSO/UC and related software and documentation files:

Category	File Name	Type	Description
Documentation	SSO-UC_README. TXT	ASCII	**Readme File**. Use this file for any pre-installation instructions, last minute changes, new instructions, and additional information to supplement the manuals. Read all sections of this file prior to following the installation instructions in the *Single Sign-On/User Context (SSO/UC) Installation Guide* (i.e., SSO-UC_INSTALLGUIDE.PDF).
	SSO-UC_INSTALL GUIDE.PDF	Binary	**Installation Guide**. Use this manual in conjunction with the Readme text file (i.e., SSO-UC_README.TXT) to install the required software.
	SSO-UC_DEPLOY GUIDE.PDF	Binary	**Deployment Guide**. This manual contains the User Manual, Programmer Manual, and Systems Management Guide information for SSO/UC.
Software	SSO/UC-related VistA M Server Patches (See Table 1-2)	ASCII	**Kernel Installation and Distribution System (KIDS) Distributions (Patches)/Software Releases** (see FORUM). Software patches for installation on the VistA M Server: • Kernel—Options, RPCs, Routines, & Files • RPC Broker—Options, RPCs, Routines, & Files • VistALink—Options, RPCs, Routines, & Files
	CCOW_Context_ Monitor.msi	Binary	(optional) **CCOW Context Monitor** (client software). VistA software for all *standard* client workstations running CCOW-enabled and SSO/UC-aware applications.

Table 1-1. Distribution files—SSO/UC client/server files

NOTE: The ISS SSO/UC Development Team developed the CCOW Context Monitor application software as an additional monitoring tool and is *not* required by the SSO/UC-related software and its functionality.

REF: The latest test version of the CCOW Context Monitor application is available for download at the following Web addresses:

http://vista.med.va.gov/kernel/sso/download.asp#all

NOTE: This manual assumes that the Sentillion Vergence Context Vault V. 3.3 (or higher), which is required for CCOW functionality, is already installed and running on the appropriate server.

Dependencies—VistA M Client/Server Patches

Kernel (i.e., Kernel Patch XU*8.0*337) is the designated custodial software package of the Infrastructure & Security Services (ISS) SSO/UC and related software. However, SSO/UC comprises/depends on multiple software patches released by several VistA M Server applications (listed by software name):

Category	Software	Version	Patch	Subject/Description
Client (for development)	RPC Broker	1.1	XWB*1.1*40	BDK32 With TCCOWRPCBroker—This client-side patch updates the Broker Development Kit (BDK). It allows developers to make their CCOW-enabled RPC Broker-based rich client applications SSO/UC-aware via the TCCOWRPCBroker component. It also enables the TRPCBroker and TCCOWRPCBroker components to establish a connection with a non-callback server (as provided with Broker Patch XWB*1.1*35). **NOTE:** This client-side patch is dependent on the server-side RPC Broker Patch XWB*1.1*35.
Server	Kernel	8.0	XU*8.0*265	3 Strikes and You Are Out—This patch enhances security by providing IP address locking functionality (terminal servers are uniquely handled). Also provides special locking security for individual users. **NOTE:** This patch is required for Kernel Patch XU*8.0*337.
			XU*8.0*284	API for Production Account Check—This patch adds two parameters to XUP with SYS or USR values that can be set to control XUP. It added the $$PROD^XUPROD() API.

Category	Software	Version	Patch	Subject/Description
			XU*8.0*337	CCOW SSO/UC Support—This patch updates Kernel authentication and authorization routines in order to enable SSO/UC and provide the VPID for SSO/UC. It also distributes the XUS ALLKEYS RPC and adds the GUI POST SIGN-ON field (#231) to the KERNEL SYSTEM PARAMETERS file (#8989.3). **NOTE:** Kernel (i.e., Kernel Patch XU*8.0*337) is the designated custodial software package of the SSO/UC-related software. This patch is dependent on Kernel Patch XU*8.0*265, because Kernel Patches XU*8.0*265 and 337 are modifying the same Kernel authentication and authorization routines. Also, Kernel Patch XU*8.0*284 (released), though not officially part of the SSO/UC Project (Iteration 1), contains an API whose need arose in discussions with developers during the SSO/UC Project (Iteration 1).
			XU*8.0*361	Proxy Application User for Re-hosting Effort—SSO/UC uses the Application Proxy user provided with this patch.
	RPC Broker	1.1	XWB*1.1*35	NON-callback Server—This patch provides local sites with the ability to control the range of ports used in connecting to joint and/or contracting facilities, useful behind firewalls. This patch contains the following: • Modified XWB LISTENER STARTER option. • Added a new XWB LISTENER STOP ALL option. • Modified RPC BROKER SITE PARAMETERS file (#8994.1). • Modified XWB LISTENER EDIT template. • New entry added to the PARAMETER DEFINITION file (#8989.51). • Modified/New routines. **NOTE:** This server-side patch is required for client-side RPC Broker Patch XWB*1.1*40.

Table 1-2. Dependencies—VistA M Server patches

REF: For specific VistA M Server patch details, please refer to the Patch Module on FORUM.

NOTE: This table only includes VistA M Server software patches required for SSO/UC; it does *not* list Commercial-Off-The-Shelf (COTS) software or other VistA/Health*e*Vet-VistA software/patches that are not directly related to SSO/UC. However, SSO/UC does depend on other underlying COTS CCOW-related software (e.g., Sentillion Vergence Context Vault).

This manual assumes that the Sentillion Vergence Context Vault V. 3.3 (or higher), which is required for CCOW functionality, is already installed and running on the appropriate server.

REF: For a list of COTS CCOW-related software, please refer to the *SSO/UC Deployment Guide*.

Installer/Developer Notes—SSO/UC Software Upgrades

All of the SSO/UC-related software has been released (e.g., executables, Zip files, and VistA M Server patches).

If you were a test site prior to the final release of SSO/UC, we have notated those installation steps/procedures that have special information based on the final software upgrades that may affect how you install the released version of the SSO/UC-related software or provide other pertinent information. The upgrade information will be displayed as follows:

UPGRADES: *Upgrade-specific instructions or information will be found here.*

In addition, we will use this section to also highlight any SSO/UC code changes that may affect development teams coding CCOW-enabled and SSO/UC-aware applications.

End-user Client Workstation Environment Requirements

NOTE: The information in this topic is directed at the Information Resource Management (IRM) or other site personnel responsible for maintaining end-user client workstations.

The following minimum software tools are required for all end-user client workstation running any CCOW-enabled and SSO/UC-aware client/server applications:

Minimum Hardware/Software Requirement	Description
Workstation Hardware	80x86-based client or server workstation.
Operating System Software	One of the following operating systems: • Microsoft Windows XP • Microsoft Windows 2000
Network Communications Software **REF:** For more information on telecommunications support, please visit the VA Office of Information and Technology (OIT) Home Page: http://vaww.va.gov/oirm/telecom/	All end-user client workstations *must* have the following network communications software and capability: • Networked client/server workstations running Microsoft's native TCP/IP stack. **NOTE:** Currently, only Winsock compliant TCP/IP protocol is supported on the LAN or remotely as Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP). You *must* use RAS (Remote Access Service) or Dialup Networking to connect to the server using PPP or SLIP. For the setup of RAS or Dialup Networking, please refer to the appropriate operating system's documentation. • Connectivity with the VistA M Server (i.e., VA Wide Area Network [WAN] connectivity). Run PING.EXE to test the connectivity. • Capability to log onto the NT network using a unique NT Logon ID.

Table 1-3. End-user client workstation minimum hardware and software tools/utilities required for SSO/UC

VistA M Server Environment

NOTE: The information in this topic is directed at the Information Resource Management (IRM) personnel located at a site.

The following minimum software tools network configuration are required on the VistA M Server running CCOW-enabled and SSO/UC-aware applications:

Minimum Software/Configuration	Description
Operating System Software	One of the following operating systems: • InterSystems Caché • Digital Standard M (DSM) V6.3-031 for OpenVMS AXP or greater **NOTE:** The VistA M Server need not be an NT system.
Fully Patched M Accounts	You should have both a development Test account and a Production account for SSO/UC software. The account(s) *must* contain the *fully* patched versions of the following software: • Kernel V. 8.0 • Kernel Toolkit V. 7.3 • RPC Broker V. 1.1 • VA FileMan V. 22.0 • VistALink V. 1.5 **NOTE:** Kernel (i.e., Kernel Patch XU*8.0*337) is the designated custodial software package for SSO/UC. However, SSO/UC comprises multiple patches and software releases from several HealtheVet-VistA applications. **REF:** For the specific software/patches required for the implementation of SSO/UC, please refer to Table 1-2 in this chapter.
Network Communications Software **REF:** For more information on telecommunications support, please visit the VA Office of Information and Technology (OIT) Home Page: http://vaww.va.gov/oirm/telecom/	The VistA M Server needs to have TCP/IP running.

Table 1-4. VistA M Server minimum software/network tools/utilities required for SSO/UC

Client workstation Environment Requirements

NOTE: The information in this topic is directed at the Enterprise Management Center (EMC) personnel responsible for maintaining the client workstations.

The following minimum hardware and software tools/utilities are required for the client workstations running CCOW-enabled and SSO/UC-aware Vista/HealtheVet-VistA applications:

Minimum Hardware/Software Requirement	Description
Workstation Hardware	80x86-based client or server workstation.
Operating System Software	One of the following operating systems: • Microsoft Windows XP • Microsoft Windows 2000
CCOW Context Monitor	This (small) rich client application runs in the background and is automatically started at system startup. It provides the current CCOW User Context identity and the ability to clear the User Context. **REF:** For installation instructions, please see the "(Optional) End-user Client Workstation Installation Instructions" topic in this manual.
CCOW-enabled and SSO/UC Application(s)	In order to have CCOW and SSO/UC functionality, the workstation *must* have at least one application that is CCOW-enabled and SSO/UC-aware, such as Computerized Patient Record System (CPRS) GUI and Care Management (CM).

Minimum Hardware/Software Requirement	Description
Network Communications Software/Capability **REF:** For more information on telecommunications support, please visit the VA Office of Information and Technology (OIT) Home Page: http://vaww.va.gov/oirm/telecom/	All client workstations *must* have the following network communications software and capability: • Networked client/server workstations running Microsoft's native TCP/IP stack. **NOTE:** Currently, only Winsock compliant TCP/IP protocol is supported on the LAN or remotely as Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP). You *must* use RAS (Remote Access Service) or Dialup Networking to connect to the server using PPP or SLIP. For the setup of RAS or Dialup Networking, please refer to the appropriate operating system's documentation. • Connectivity with the VistA M Server (i.e., VA Wide Area Network [WAN] connectivity). Run PING.EXE to test the connectivity. • Capability to log onto the NT network using a unique NT Logon ID.

Table 1-5. Client workstation minimum hardware and software tools/utilities required for CCOW-enabled and SSO/UC-aware applications

2. VistA M Server Installation Instructions

The installation instructions in this section are directed at the Information Resource Management (IRM) personnel located at a site and are applicable for the Test/Production accounts in the DSM or Caché environments.

REF: For VistA M Server platform requirements, please refer to the "VistA M Server Environment" topic in the "Pre-Installation Instructions" chapter in this manual.

1. Confirm/Obtain VistA M Server Distribution Files *(recommended)*

The following files are needed to install the SSO/UC-related VistA M Server software:

Category	File Name	Type	Description
Documentation	SSO-UC_ README.TXT	ASCII	**Readme Text File.** This file provides any pre-installation instructions, last minute changes, new instructions, and additional information to supplement the manuals. Read all sections of this file *prior* to following the installation instructions in the *Single Sign-On/User Context (SSO/UC) Installation Guide* (i.e., SSO-UC_INSTALLGUIDE.PDF).
	SSO-UC_ INSTALLGUIDE. PDF	Binary	**Installation Guide.** Use in conjunction with the Readme text file (i.e., SSO-UC_README.TXT).
Software	XU*8.0*265	ASCII	**Kernel Patch XU*8.0*265.** KIDS build for Kernel Patch XU*8.0*26 (released on 12/12/05, required for Kernel Patch XU*8.0*337, see Table 1-2 for patch details). Follow normal procedures to obtain and install this released patch (see FORUM).
	XU*8.0*337	ASCII	**Kernel Patch XU*8.0*337.** KIDS build for Kernel Patch XU*8.0*337 (released on 12/22/05, see Table 1-2 for patch details). Follow normal procedures to obtain and install this released patch (see FORUM).
	XU*8.0*361	ASCII	**Kernel Patch XU*8.0*361.** KIDS build for Kernel Patch XU*8.0*361 (released on 01/31/06, see Table 1-2 for patch details). Follow normal procedures to

Category	File Name	Type	Description
			obtain and install this patch (see FORUM).
	XWB*1.1*35	ASCII	**RPC Broker Patch XWB*1.1*35.** KIDS build for RPC Broker Patch XWB*1.1*35 (released on 01/20/05, see Table 1-2 for patch details). Follow normal procedures to obtain and install this patch (see FORUM).
	XWB*1.1*40	ASCII	**RPC Broker Patch XWB*1.1*40.** KIDS build for RPC Broker Patch XWB*1.1*40 (released on 01/20/05, see Table 1-2 for patch details). Follow normal procedures to obtain and install this released patch (see FORUM).

Table 2-1. Distribution files—SSO/UC-related VistA M Server files

2. Retrieve VistA M Server Patches *(required)*

Several VistA M Server-side patches are required for SSO/UC installation (see Table 2-1). You should have these patches readily available so that you can apply them later in the installation process. You can obtain all released SSO/UC-related VistA M Server-side patches from the Patch module on FORUM or through normal procedures.

NOTE: Kernel (i.e., Kernel Patch XU*8.0*337) is the designated custodial software package for SSO/UC-related software. However, SSO/UC comprises multiple patches and software releases from several VistA/HealtheVet-VistA applications.

REF: For the specific VistA M Server software patches required for the implementation of SSO/UC, please refer to Table 1-2 in Chapter 1, "Pre-Installation Instructions" in this manual.

3. Stop Any CCOW-enabled and SSO/UC-aware Software Running on the VistA M Server *(required)*

No VistA client/server software that is CCOW-enabled and SSO/UC-aware should be running while the SSO/UC installation on the VistA M Server is taking place.

4. Verify KIDS Install Platform *(required)*

Verify that the Kernel Installation and Distribution System (KIDS) platform on your system is ready to install VistA M Server patches.

A. Verify Host File Server (HFS) Device in the DEVICE File (#3.5)

Verify that you have a Host File Server (HFS) device in the DEVICE file (#3.5) named "**HFS**". If you have performed KIDS installations on the VistA M Server before, you probably already have an appropriate HFS device set up. If you don't have an entry for this device, you *must* create one.

REF: For information on how to create an HFS device, please refer to Chapter 18, "Host Files," in the *Kernel Systems Manual*.

B. Verify Null Device in the DEVICE File (#3.5)

Verify that you have a Null device in the DEVICE file (#3.5) named "NULL" (or whose mnemonic is named "NULL").

You can have other devices with similar names, but one device is needed whose name or mnemonic is "NULL." The subtype should be a "P-" subtype (e.g., P-OTHER), the margin should be a minimum of 80, and the page length should be a minimum of 60. Sample setups:

Caché or DSM for OpenVMS Null Device Setup Example

```
NAME: NULL                         $I: _NLA0:
  ASK DEVICE: NO                   ASK PARAMETERS: NO
  SIGN-ON/SYSTEM DEVICE: NO        LOCATION OF TERMINAL: Bit Bucket
  SUBTYPE: P-OTHER                 TYPE: TERMINAL
```

Caché/NT Null Device Setup Example

```
NAME: NULL                         $I: //./nul
  ASK DEVICE: NO                   ASK PARAMETERS: NO
  SIGN-ON/SYSTEM DEVICE: NO        LOCATION OF TERMINAL: BIT BUCKIT
  SUBTYPE: P-OTHER                 TYPE: TERMINAL
```

P-OTHER Terminal Type Setup Example

```
NAME: P-OTHER                      RIGHT MARGIN: 132
  FORM FEED: #                     PAGE LENGTH: 64
  BACK SPACE: $C(8)                DESCRIPTION: General prntr (132)
```

5. Install SSO/UC-related VistA M Server Patches *(required)*

Make sure that the Kernel, Kernel Toolkit, RPC Broker, VA FileMan, and VistALink software is fully patched. Patches must be installed in their published sequence.

The SSO/UC-related VistA M Server patches are listed in Table 1-2. All VistA M Server patches are distributed in Kernel V. 8.0 KIDS format. Follow the normal procedures to obtain released patches.

REF: For more information on these patches, please refer to Table 1-2 in this manual or the Patch Module on FORUM.

Using KIDS, load and install the SSO/UC-related VistA M Server patches on all VistA M systems to which any CCOW-enabled and SSO/UC-aware VistA/HealtheVet-VistA applications will be connecting (i.e., VistA M Server Test and Production accounts).

Follow the instructions under the "Installation Instructions" section in the patch description in order to install each patch.

REF: For more information on KIDS, please refer to the KIDS section in the *Kernel Systems Manual* located on the VDL at the following Web address:

http://www.va.gov/vdl/Infrastructure.asp?appID=10

Congratulations! You have now completed the installation of SSO/UC-related software on the VistA M Server.

3. (Optional) End-user Client Workstation Installation Instructions

The installation instructions in this section are optional and are directed at the Information Resource Management (IRM) personnel responsible for maintaining the end-user client workstations and are applicable for the Client/Server environment.

REF: For client workstation platform requirements, please refer to the "End-user Client Workstation Environment Requirements" topic in the "Pre-Installation Instructions" chapter in this manual.

UPGRADES: If you have previously installed the CCOW Context Monitor on the workstation and it is currently running in the background, do the following:

1. Stop the CCOW Context Monitor—To determine if the Context Monitor is running, look for the CCOW Context Monitor icon in the client workstation's system tray. To stop it, right click (left click for left-handed users) on the CCOW Context Monitor icon and select **Exit** from the menu list. The **Exit** command exits the menu display *and* shuts down the CCOW Context Monitor application running in the background.
2. Uninstall the CCOW Context Monitor using Microsoft Windows Add/Remove Programs on the Control Panel.

1. Confirm/Obtain Client/Server Workstation Distribution Files *(recommended)*

The following files are needed to install the SSO/UC client workstation software:

Category	File Name	Type	Description
Documentation	SSO-UC_ README.TXT	ASCII	**Readme Text File.** This file provides any pre-installation instructions, last minute changes, new instructions, and additional information to supplement the manuals. Read all sections of this file prior to following the installation instructions in the *Single Sign-On/User Context (SSO/UC) Installation Guide* (i.e., SSO-UC_INSTALLGUIDE.PDF).
	SSO-UC_ INSTALLGUIDE.PDF	Binary	**Installation Guide.** Use in conjunction with the Readme text file (i.e., SSO-UC_README.TXT).

Category	File Name	Type	Description
Software	CCOW_Context_ Monitor.msi	Binary	(optional) **CCOW Context Monitor** (client software). VistA software for all standard end-user client workstations running CCOW-enabled and SSO/UC-aware applications.

Table 3-1. Distribution files—SSO/UC client workstation files

NOTE: The ISS SSO/UC Development Team developed the CCOW Context Monitor application software as an additional monitoring tool and is *not* required by the SSO/UC-related software and its functionality.

REF: The latest test version of the CCOW Context Monitor application is available for download at the following Web addresses:

http://vista.med.va.gov/kernel/sso/download.asp#all

2. Create an SSO/UC Staging Folder *(required)*

UPGRADES: If you have previously created a **<STAGING_FOLDER>**, skip to Step #3 that follows.

Create a staging folder in a good working location on the file system of each end-user client workstation on which you are deploying the CCOW Context Monitor. This will be referred to as the **<STAGING_FOLDER>** for the rest of the instructions. This will be the location in which various SSO/UC folders/files will be prepared prior to installation.

3. Copy/Move the CCOW_Context_Monitor.msi File *(required)*

Copy/Move the CCOW Context Monitor.msi file (i.e., CCOW_Context_Monitor.msi) from the software distribution source to the **<STAGING_FOLDER>** that you created in Step #2.

4. Run the CCOW Context Monitor Install Wizard *(required)*

NOTE: We recommend that you shut down all other Microsoft Windows-based applications running on the client workstation. In particular, you *must not* be running *any* CCOW-enabled and SSO/UC-aware applications during the installation.

Double click on the CCOW_Context_Monitor.msi file (see Step #3) or do the following:

1. Go to the **Start** menu.
2. Go to the **Run** menu.
3. Press the **Browse** button and navigate to the **<STAGING_FOLDER>** you created in Step #2.

4. Highlight/Select the CCOW_Context_Monitor.msi file.
5. Press the **Open** button.
6. Press **OK**.

Follow the install wizard prompts to install the CCOW Context Monitor. We recommend that you accept the default settings.

After the installation completes, start the CCOW Context Monitor by either of the following methods:

- Reboot/Restart the client workstation.
- Go to the Microsoft Windows Startup folder and select ContextMonST from the list:
    1. Go to the **Start** menu.
    2. Go to the **Programs** menu.
    3. Go to the **Startup** menu.
    4. Select **ContextMonST** from the list.

The CCOW Context Monitor will start up and run in the background.

5. Test the CCOW Context Monitor and SSO/UC Functionality *(recommended)*

After the CCOW Context Monitor install wizard finishes the installation, test the CCOW Context Monitor.

REF: For a detailed description of and the functionality provided by the CCOW Context Monitor, please refer to the "CCOW Context Monitor" topic in Chapter 2, "SSO/UC VistA Applications/Modules," in Part I, "User Guide," in the *SSO/UC Deployment Guide*.

Congratulations! You have now completed the installation and configuration of SSO/UC-related software on the Client Workstation.

Upon completing the installation of the SSO/UC-related software on the VistA M Server and Client Workstation, you are now ready to develop/run VistA client/server-based applications that are CCOW-enabled and SSO/UC-aware.