|  |  |  |
| --- | --- | --- |
|  |  |  |

Department of Veterans Affairs

Veterans Crisis Line (VCL)

Installation Guide



**Version 0.6**

**December 2014**

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 12/01/2014 | 0.6 | Technical edit. Added figure captions and two new screens to section 6. | REDACTED |
| 6/25/14 | 0.5 | Updated content and formatting | REDACTED |
| 6/12/14 | 0.4 | Updated with current installation instructions | REDACTED |
| 05/08/2014 | 0.3 | Removed Other Considerations section, which included 2008 server references. Added pre-prod links to Section 3.1, General Installation Flow. | REDACTED |
| 05/06/2014 | 0.2 | Modified web installation content to meet AITC standards. | REDACTED |
| 3/25/2014 | 0.2 | Added Raj’s SSRS content. Added AITC content to pre-installation section. Reviewed and incorporated comments from SQA. | REDACTED |
| 02/18/2014 | 0.2 | Add MDWS installation instructions | REDACTED |
| 02/06/14 | 0.2 | Added instructions on how to obtain VCL code base. | REDACTED |
| 6/3/2013 | 0.1 | Created template | REDACTED |

Table of Contents

[Introduction 8](#_Toc404156165)

[1.1. Overview 8](#_Toc404156166)

[1.2. Audience 8](#_Toc404156167)

[1.3. Scope 8](#_Toc404156168)

[1.4. Veterans Crisis Line 8](#_Toc404156169)

[1.5. Using This Manual 8](#_Toc404156170)

[1.6. How Much Do I Need to Install? 9](#_Toc404156171)

[1.7. Related Documentation 9](#_Toc404156172)

[2. Preinstallation 11](#_Toc404156173)

[2.1. Preinstallation Steps 11](#_Toc404156174)

[2.2. System Backup 15](#_Toc404156175)

[2.3. Retrieving Files from Staging Areas 15](#_Toc404156176)

[2.3.1. Database Staging Area 15](#_Toc404156177)

[2.3.2. Application Staging Area 15](#_Toc404156178)

[3. Installation Prerequisites 16](#_Toc404156179)

[3.1. SSL Setup 18](#_Toc404156180)

[3.2. General VCL Installation Flow 19](#_Toc404156181)

[3.3. MDWS installation 39](#_Toc404156182)

[3.4. System Requirements 41](#_Toc404156183)

[4. Backout Plan 42](#_Toc404156184)

[5. Post Installation Instructions 44](#_Toc404156185)

[6. Installing and Configuring the SQL Server Reports Server (SSRS) Component 45](#_Toc404156186)

[6.1. Audience 45](#_Toc404156187)

[6.2. Pre-Requisites 45](#_Toc404156188)

[6.3. Configuring the Reports Server (Includes SSL) 46](#_Toc404156189)

[6.4. Defining the Reporting Web Project 51](#_Toc404156190)

[6.5. Reporting Services SSL Configuration 59](#_Toc404156191)

[6.6. Uploading Previously Developed “Sample Reports” to the Server 59](#_Toc404156192)

[7. Patching the Production Environment with Updated Code 60](#_Toc404156193)

[8. Troubleshooting 62](#_Toc404156194)

[8.1. Rollback Instructions 62](#_Toc404156195)

[9. FAQ 63](#_Toc404156196)

List of Figures

[Figure 1: VCL Application Flow 21](#_Toc405203751)

[Figure 2: VCL Installed Components 23](#_Toc405203752)

[Figure 3: VCL Add Features Wizard 24](#_Toc405203753)

[Figure 4: VCL Installing Web Services Enhancements 3.0 – select Runtime option 25](#_Toc405203754)

[Figure 5: Installing Web Services Enhancements 3.0 – Click Finish to complete installation 26](#_Toc405203755)

[Figure 6: Unpack VCL Code Archive 27](#_Toc405203756)

[Figure 7: IIS Manager 28](#_Toc405203757)

[Figure 8: VCL Site Breakout 29](#_Toc405203758)

[Figure 9: VCL Site Breakout Expanded 29](#_Toc405203759)

[Figure 10: SSL Settings 30](#_Toc405203760)

[Figure 11: Application Pools 30](#_Toc405203761)

[Figure 12: Edit Application Pool settings 31](#_Toc405203762)

[Figure 13: CrisisCenter Properties 32](#_Toc405203763)

[Figure 14: Permissions for CrisisCenter 33](#_Toc405203764)

[Figure 15: Locations 33](#_Toc405203765)

[Figure 16: Enter the Object Names to Select 34](#_Toc405203766)

[Figure 17: Check Names 34](#_Toc405203767)

[Figure 18: Default Permissions 35](#_Toc405203768)

[Figure 19: IIS Manager, CrisisCenter Virtual directory 36](#_Toc405203769)

[Figure 20: Edit Application 37](#_Toc405203770)

[Figure 21: Connect As dialogue 37](#_Toc405203771)

[Figure 22: Crisis Center Hotline Login 39](#_Toc405203772)

[Figure 23: CrisisCenter Response 40](#_Toc405203773)

[Figure 24: CrisisCenter Administrator 40](#_Toc405203774)

[Figure 25: Unpack VCL Code Archive 45](#_Toc405203775)

[Figure 26: Reporting Services Configuration Connection 48](#_Toc405203776)

[Figure 27: Reporting Services Configuration Manager 49](#_Toc405203777)

[Figure 28: Specify a Server Name 49](#_Toc405203778)

[Figure 29: Report Server Status 50](#_Toc405203779)

[Figure 30: SSL Certificate and SSL Port 50](#_Toc405203780)

[Figure 31: SSL Certification Information 51](#_Toc405203781)

[Figure 32: Add Report Manager URL 51](#_Toc405203782)

[Figure 33: UpdatingSSL Certificates 52](#_Toc405203783)

[Figure 34: Create a Datasource 53](#_Toc405203784)

[Figure 35: VCL Datasource 54](#_Toc405203785)

[Figure 36: Generate Model 55](#_Toc405203786)

[Figure 37: VCL Model 56](#_Toc405203787)

[Figure 38: System User 57](#_Toc405203788)

[Figure 39: New Role Assignment 57](#_Toc405203789)

[Figure 40: Edit Role Assignment 58](#_Toc405203790)

[Figure 41: Security 58](#_Toc405203791)

[Figure 42: Properties 59](#_Toc405203792)

[Figure 43: Veterans Crisis Line – Custom Reports 60](#_Toc405203793)

[Figure 44: Upload File 61](#_Toc405203794)

[Figure 45: Change Order Request Email 63](#_Toc405203795)

# Introduction

This Veterans Crisis Line (VCL) Installation Guide provides information for Information Resource Management (IRM) personnel to install and configure the components of the VCL application.

## Overview

The Office of Mental Health Services (OMHS) is currently managing a web-based application (herein referred to as VCL) utilized by their confidential, free 24-hours hotline staff to make referrals to the appropriate field-based Suicide Prevention Coordinators (SPCs).

OMHS is requesting OIT to assist OMHS to enhance, deploy and support the existing Veterans Crisis Line application and hardware platform utilizing Information Technology (IT) best practices and procedures rather than maintaining the existing ad-hoc environment.

## Audience

This document has been prepared for system administrators and database administrators who need to set up development, pre-production and/or production environments at the Austin Information Technology Center (AITC). It is presumed that readers of this document understand basic concepts of the VCL environments as well as any system specialties that might pertain to the installation of the VCL software.

## Scope

This Installation Guide includes steps for installing the Pre-Prod environment. Assumptions for installation include the following:

* Pre-installation steps have been completed.
* 9957’s have been submitted 30 days prior to need date for each environment
* All backups have been performed
* All files have been placed into the appropriate staging area
* Application server certificates have been installed.

## Veterans Crisis Line

## Using This Manual

This manual guides the reader through a very specific order for installing and configuring the various components of VCL.

## How Much Do I Need to Install?

Depending on your purposes for installing VCL components, you may not need to install all of the components described in this Installation Guide. Please follow these guidelines for determining which components you should install:

This Guide also covers the install from a total “ground-up” perspective. This involves the following additional steps:

* Restoring the VCL database from a backup file.
* Obtaining and installing the VCL code.
* Installing the appropriate version of SQL Server Reporting Services.
* Installing the correct version and configuration of IIS.
* Installing the correct version of MDWS web service.

## Related Documentation

Refer to the following documentation for additional information about VCL.

The documentation will be in the form of Adobe Acrobat files.

Documentation can also be found on the [VA Software Documentation Library](http://www4.va.gov/vdl/).

|  |  |
| --- | --- |
| File Name | Description |
| VCL Production Operations Manual (POM).PDF | Includes system and operational description for VCL, information about routine operations, and contingency planning. |
| VCL\_Release Notes.PDF | Release notes on new features and functionality |
| VCL\_User Guide.PDF | VCL User Guide |
| VCL\_Installation Guide.PDF | Installation Guide for installation in various environments |

*This page intentionally left blank for double-sided printing.*

# Preinstallation

The following sections include steps required to setup the development environment.

## Preinstallation Steps

The following preinstallation steps need to be completed for the development environment:

**Group Account Creation**

1. Verify/Create Security Groups for Report Viewer and Manager (9957 or ePAS).

**This function is now complete for all environments**

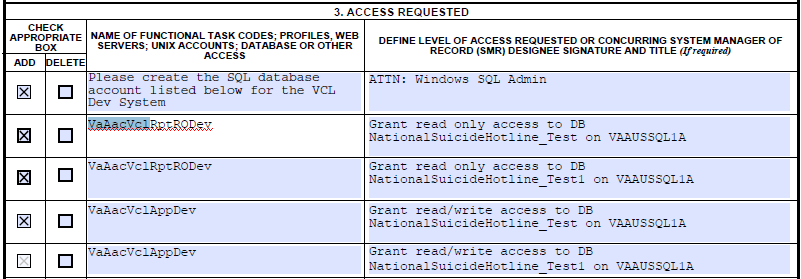
* 1. Create the Groups used for User Management Access based on the specific environment and functions.
  2. Groups Created
     1. Dev
        1. VCLREPORTMANAGER\_DEV
        2. VCLREPORTVIEWER\_DEV
     2. Preproduction
        1. VCLREPORTMANAGER\_PPD
        2. VCLREPORTVIEWER\_PPD
     3. Production
        1. VCLREPORTMANAGER
        2. VCLREPORTVIEWER



1. Submit request to grant permissions to the Security Groups created:

**This function is now complete for Development**

* 1. Granting permissions to these groups allow individuals to be added to the Security Groups rather than making multiple changes on the servers. Permissions and titles are specific to the environment, including the actual names of the database. These must be completed after the databases have been created.
  2. Permissions Created so far:
     1. Development
        1. VCLREPORTMANAGER\_DEV
           1. On the database server VAAUSSQL1a: Read permission on DB: "NationalSuicideHotline\_Test1" R\W on DB's:VCLReportServer and VCLReportServerTempDB
           2. On the VAAUCVCLAPP80 in SQL Server Reporting Service Grant the following roles: Browser, Report Builder
        2. VCLREPORTVIEWER\_DEV
           1. On the database server VAAUSSQL1a: Read permissions on DB's: VCLReportServerTempDB, VCLReportServer and "NationalSuicideHotline\_Test1"
           2. On the VAAUCVCLAPP80 in SQL Server Reporting Service Grant the following roles: Browser

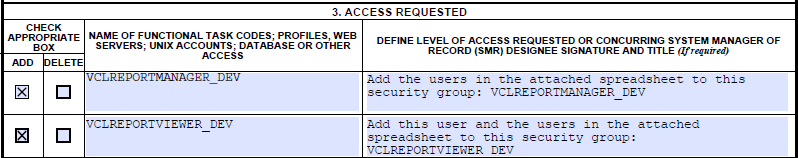


1. Submit request to add users to appropriate security groups (9957 or ePAS):

**This function is now complete for Development.**

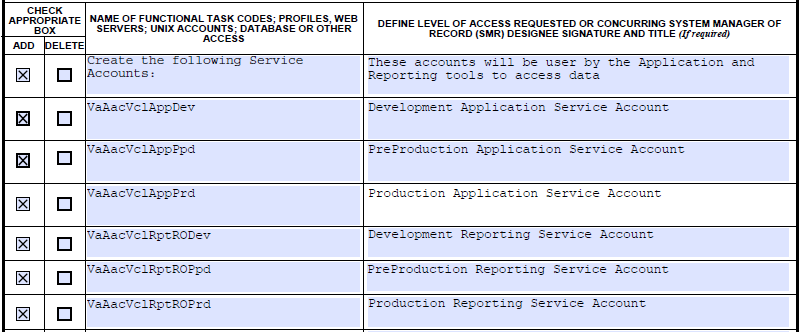
***Note:*** *Developers have requested and been individually granted elevated privileges in the development environment. Elevated privileges are restricted to EO AITC Administrators in other environments.*

REDACTED

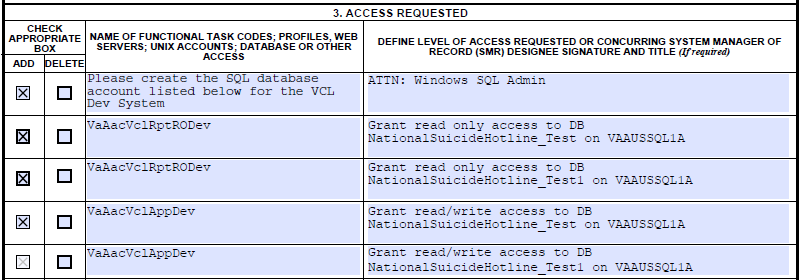


**Service Account Creation**

1. Verify/Create Application Service Accounts (9957 or ePAS) – **This function is now complete for all environments**
   1. Create the accounts used for the application to connect to the database based on the specific environment and functions.
   2. Service Accounts Created
      1. Dev
         1. VaAacVclAppDev - Development Application Service Account
         2. VaAacVclRptRODev - Development Reporting Service Account
      2. Preproduction
         1. VaAacVclAppPpd - PreProduction Application Service Account
         2. VaAacVclRptROPpd - PreProduction Reporting Service Account
      3. Production
         1. VaAacVclAppPrd - Production Application Service Account
         2. VaAacVclRptROPrd - Production Reporting Service Account



1. Submit request to grant permissions to the Security Groups created: **This function is complete for Development**
   1. Granting permissions to these groups allow the application to connect to the database. Permissions and titles are specific to the environment, including the actual names of the database. These must be completed after the databases have been created.
   2. Permissions Created so far:
      1. Dev
         1. VaAacVclAppDev
            1. Grant read/write access to DB NationalSuicideHotline\_Test on VAAUSSQL1A
            2. Grant read/write access to DB NationalSuicideHotline\_Test1 on VAAUSSQL1A
         2. VaAacVclRptRODev
            1. Grant read only access to DB NationalSuicideHotline\_Test on VAAUSSQL1A
            2. Grant read only access to DB NationalSuicideHotline\_Test1 on VAAUSSQL1A



## System Backup

Austin Information Technology Center (AITC) system backup procedures include the following:

Backing up the system

VMWARE Consolidated BACKUP

Request snapshot of entire server image. Snapshots are only completed upon request and are deleted after eight hours.

Backup of the database

***Note:*** *Full backups are performed on the system every Friday. Differential backups are performed daily.*

## Retrieving Files from Staging Areas

### Database Staging Area

The VCL Development team drops files for the Dev and PPD instance here: vaausvclapp80\vcl. Production Data Transfer will be handled according to protocols defined in a separate “Data Transfer Agreement.”

### Application Staging Area

The VCL Development team drops files for the application server here: vaausvclapp80\vcl.

# Installation Prerequisites

The following preinstallation requirements apply for users who are installing VCL:

* Windows server needs to be installed on to the target environment.
* The environment will vary based on utilization (PPD).
* Technical Manager / Configuration Manager has submitted all the firewall rules.
* Sufficient disk space is available on the application server as specified by AITC
* Database Administrator has approved 9957’s to create application accounts and roles
* Microsoft Web Service Extension 3.5
* Microsoft .Net Framework 4.0, which can be downloaded from <http://www.microsoft.com/en-us/download/details.aspx?id=17718>.
* IIS 7
  + MDWS can be installed in a new virtual directory.
* MDWS installation reference, located at <http://vaww.oed.portal.va.gov/projects/vet_crisis_line_enhancements/Library/User%20Documentation%20and%20National%20Release/mwvs2_0ig.doc>.
* Windows Server 2008 with IIS 7.0.
  + Install Microsoft .NET 3.5.1
  + Install Static Content
* A shared SQL Server Database is to be utilized. Here are the desired version specifics:
  + Database Version 10.0.1600.22 (Note, this is the SQL Server 2008 Non-R2 version)
* The SQL Server Management Studio is will be installed on the PPD Servers. Here are the version specifics:

|  |
| --- |
| * Microsoft SQL Server Management Studio 10.0.1600.22 ((SQL\_PreRelease).080709-1414 ) * Microsoft Data Access Components (MDAC) 6.1.7601.17514 (win7sp1\_rtm.101119-1850) * Microsoft MSXML 2.6 3.0 4.0 5.0 6.0 * Microsoft Internet Explorer 9.10.9200.16750 * Microsoft .NET Framework 2.0.50727.5472 * Operating System 6.1.7601 |

* SQL Server Reporting Services (SSRS) is to be installed on an application server. In the PPD instances, this will be installed on the only Application Server. In PRD, this should be installed on a server selected based on load balancing needs. The SSRS version as well as the Business Intelligence Development Studio version details are listed below:

|  |
| --- |
| * Microsoft Visual Studio 2008 Version 9.0.30729.1 SP * Microsoft .NET Framework Version 3.5 SP1 * Installed Edition: IDE Standard * Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB945282) * Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB946040) * Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB946308) * Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB946344) * Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB946581) * Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB947173) * Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB947540) * Hotfix for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB947789) * Security Update for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB2251487) * Security Update for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB2669970) * Security Update for Microsoft Visual Studio 2008 Shell (integrated mode) - ENU (KB972222) * SQL Server Analysis Services * Microsoft SQL Server Analysis Services Designer * Version 10.50.4260.0 * SQL Server Integration Services * Microsoft SQL Server Integration Services Designer * Version 10.0.1600.22 ((SQL\_PreRelease).080709-1414 ) * SQL Server Reporting Services * Microsoft SQL Server Reporting Services Designers * Version 10.0.1600.22 |

## SSL Setup

The VCL will provide PII information. To be complaint with government, VCL will encrypt all communication between client browser and server.

VCL has a total of three web sites. One requires a signed certificate. The SSL web site will have three sub-sites, which will be the three VCL web applications.

AITC will take responsibility for the SSL setup.

Dev

REDACTED

Pre-Prod

REDACTED

Prod

REDACTED

## General VCL Installation Flow

The following flow diagram illustrates an overview of the basic information flow of the application. This installation does not include the VistA servers, only verifying the MDWS-VistA connection.



Figure 1: VCL Application Flow

**IIS Installation Settings**

1. Verify IIS is installed with default settings with the following exceptions:
   1. Install Microsoft .NET 3.5.1
   2. Install Static Content
   3. Install Web Services Enhancements 3.0
   4. Verify the ASP.NET Session State Service is set to a startup type of Automatic, and is running.

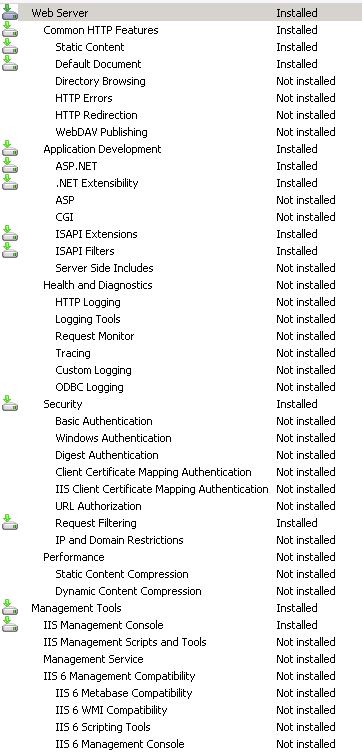
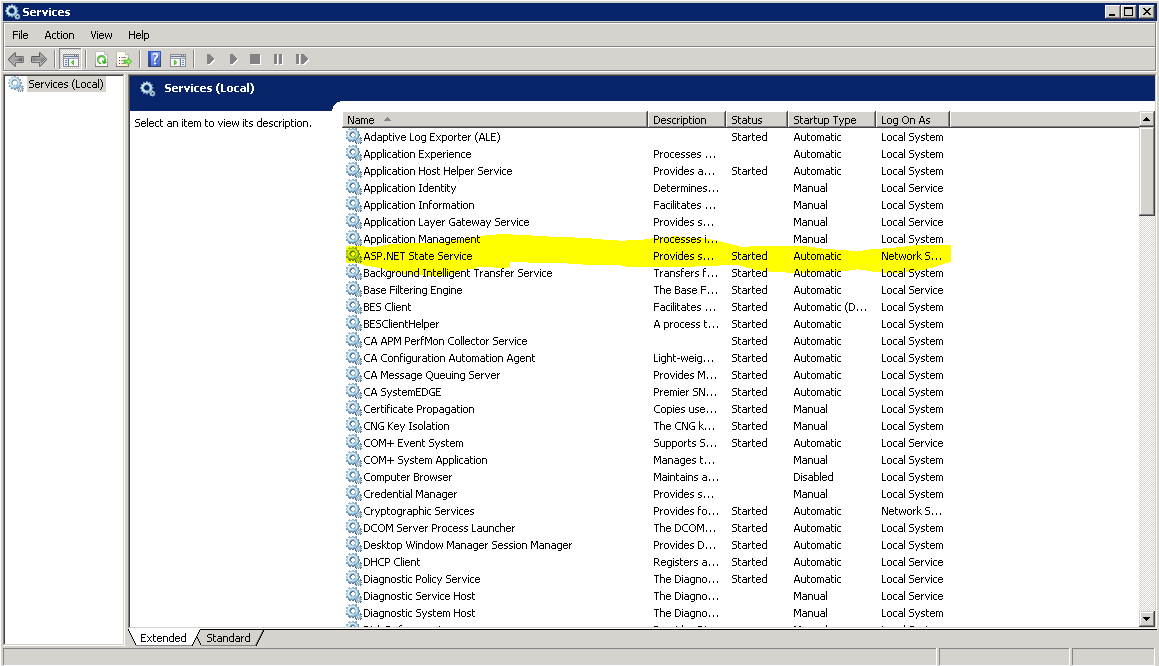


Figure 2: VCL Installed Components

**IIS Installed Components**

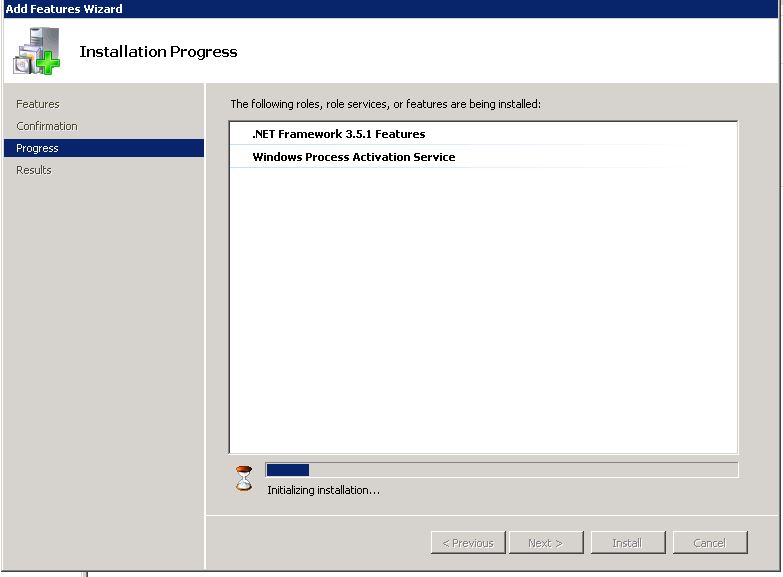


Figure 3: VCL Add Features Wizard

**IIS Additional Components**

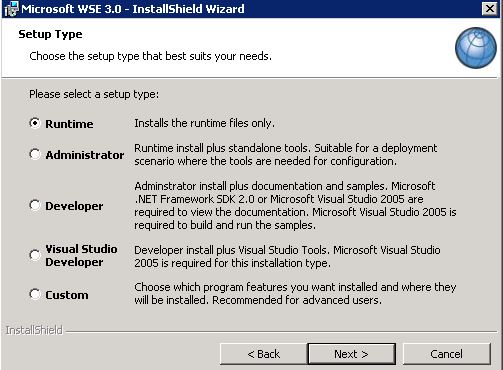


Figure 4: VCL Installing Web Services Enhancements 3.0 – select Runtime option

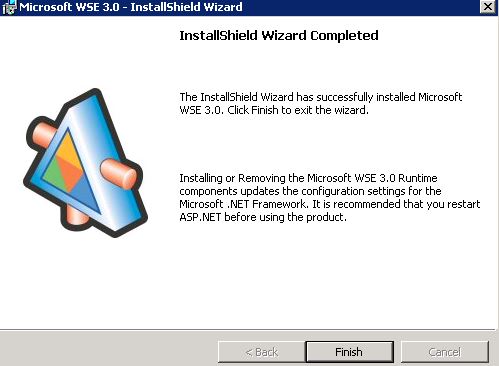


Figure 5: Installing Web Services Enhancements 3.0 – Click Finish to complete installation

**Locate VCL Code**

1. The VCL code will be uploaded onto the dev server in the location vaausvclapp80\vcl\vcl-####.zip. It will be in an archive, with a naming convention that identifies the version, and when unpacked will have a directory structure similar to the following:

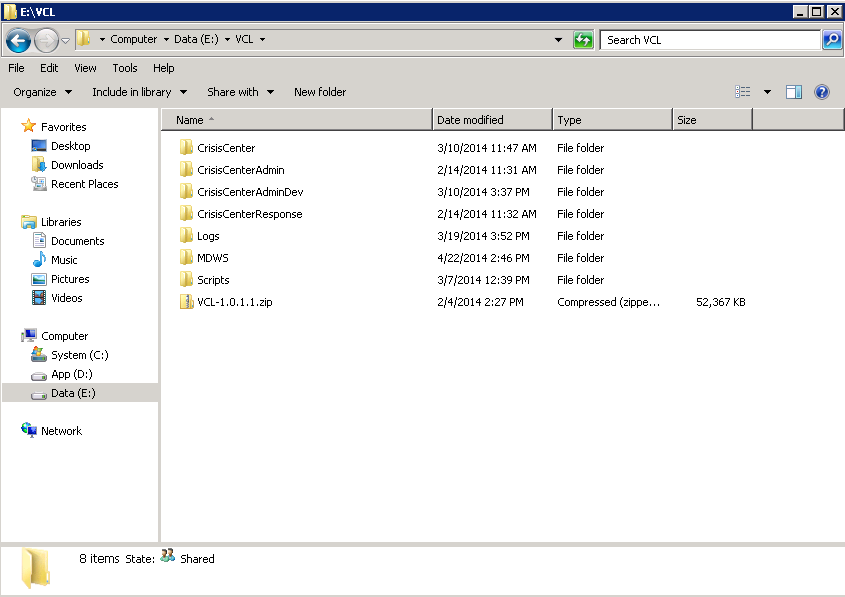


Figure 6: Unpack VCL Code Archive

Unpack the VCL code archive to E:\VCL. The folder structure should look similar to the following:

**Create and set up VCL web sites**

1. Open IIS Manager.

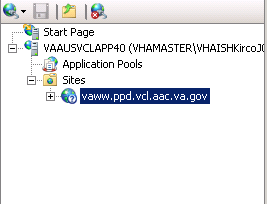


Figure 7: IIS Manager

1. In IIS Manager, go to IIS -> Authentication
2. Select "Anonymous Authentication" then select "Edit"
3. Under the "Edit Anonymous Authentication Credentials" window, make sure "Application Pool Identity" is selected.
4. Rename default site to server website name.
5. There are three applications to be created under the server website name. Right-click the server website name, and select “Add Application”

Please note that the creation of the web sites will also create the application pools, which is detailed in step b under the creation of each web application (steps 5, 6, and 7).

1. Fill in the following information for the CrisisCenter web application:
   1. Site name: CrisisCenter
   2. Application pool: CrisisCenter
   3. Physical path: E:\VCL\CrisisCenter
2. Fill in the following information for the Response web application:
   1. Site name: Response
   2. Application pool: Response
   3. Physical path: E:\VCL\CrisisCenterResponse
3. Fill in the following information for the Admin web application:
   1. Site name: Admin
   2. Application pool: Admin
   3. Physical path: E:\VCL\CrisisCenterAdmin
4. IIS Manager should look similar to the following when you are done:

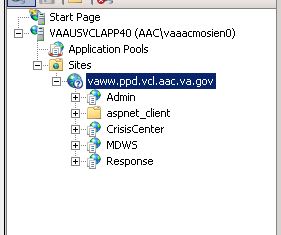


Figure 8: VCL Site Breakout

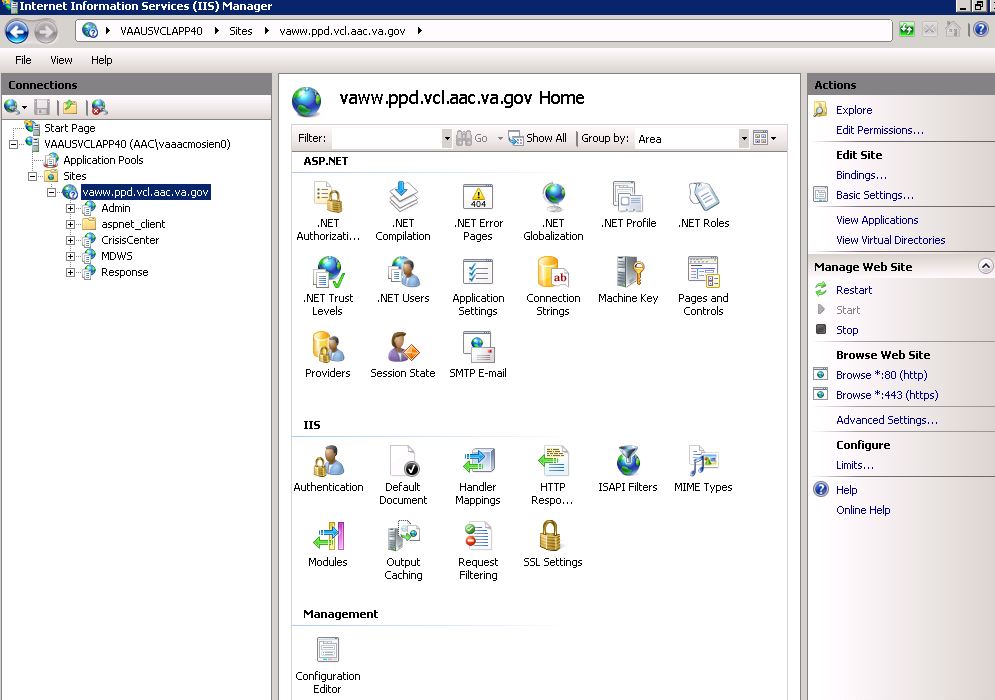


Figure 9: VCL Site Breakout Expanded

**Require SSL**

1. Add the HTTPS bindings to the website certificate using whatever process you have in place to accomplish this.
2. Select the newly created website, then double-click SSL Settings. Select Require SSL, and click Apply.

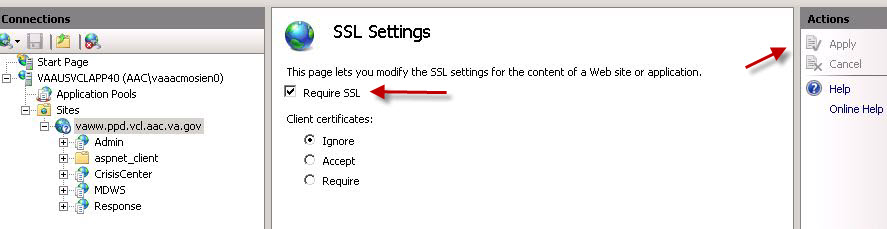


Figure 10: SSL Settings

**Modify application pools**

1. In IIS Manager, click Application Pools

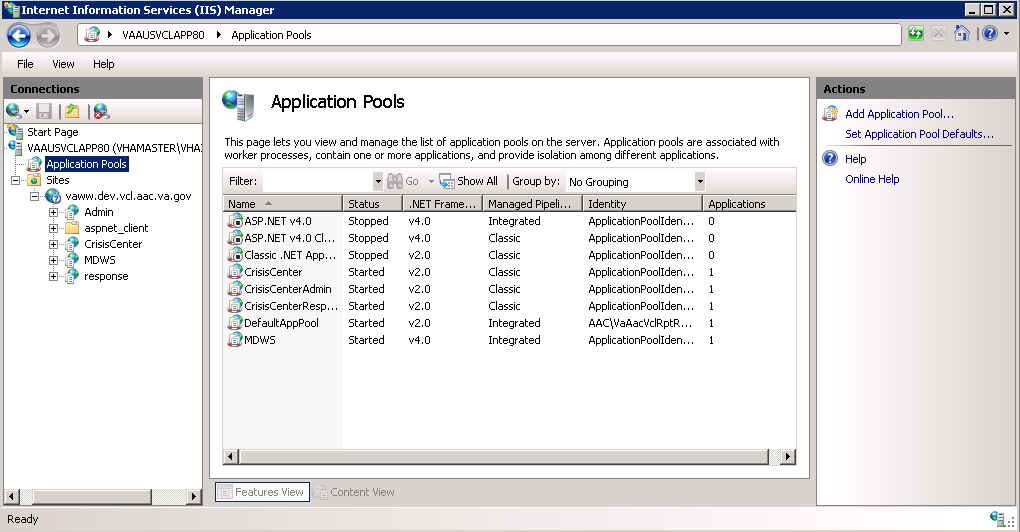


Figure 11: Application Pools

1. Double-click the CrisisCenter application pool, and change the Managed Pipeline Mode from Integrated to Classic. Click “OK” when done
2. Double-click the Response application pool, and change the Managed Pipeline Mode from Integrated to Classic. Click “OK” when done
3. Double-click the Admin application pool, and change the Managed Pipeline Mode from Integrated to Classic. Click “OK” when done

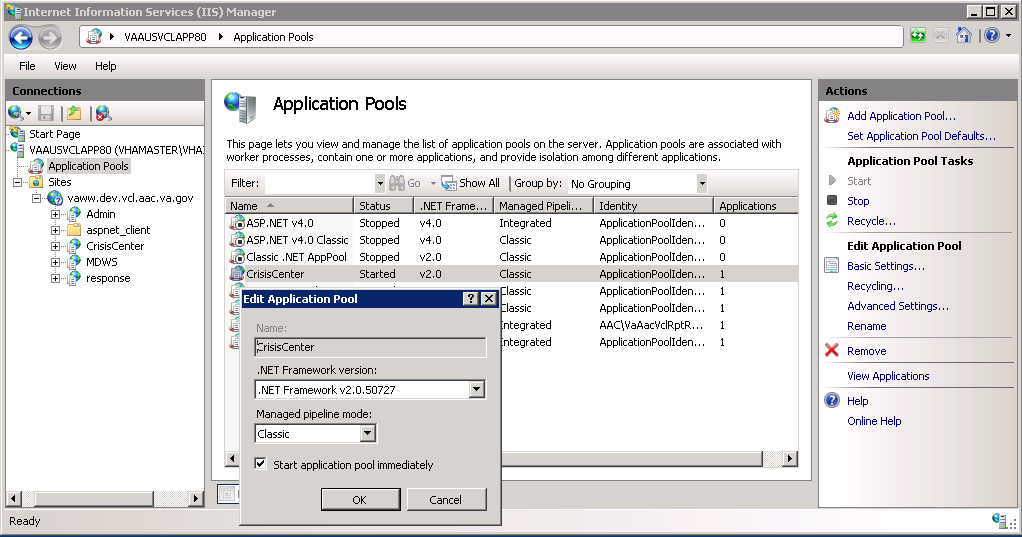


Figure 12: Edit Application Pool settings

**CrisisCenter application pool permissions to the appropriate file system folder**

1. Give the CrisisCenter application pool file system permissions to access the CrisisCenter code. Open Windows Explorer, navigate to E:\VCL\, right-click the CrisisCenter folder, select Properties, and select the Security tab.

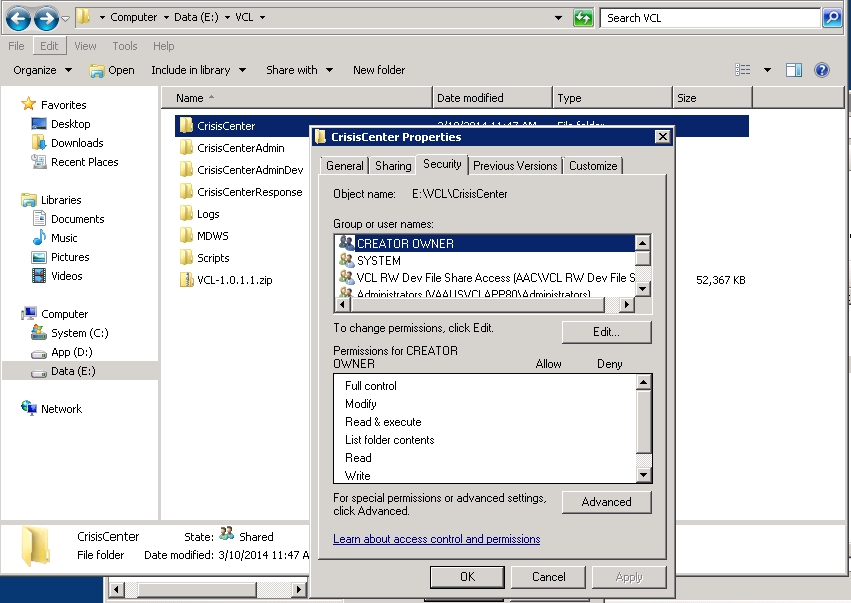


Figure 13: CrisisCenter Properties

1. Click the Edit button, then click Add.

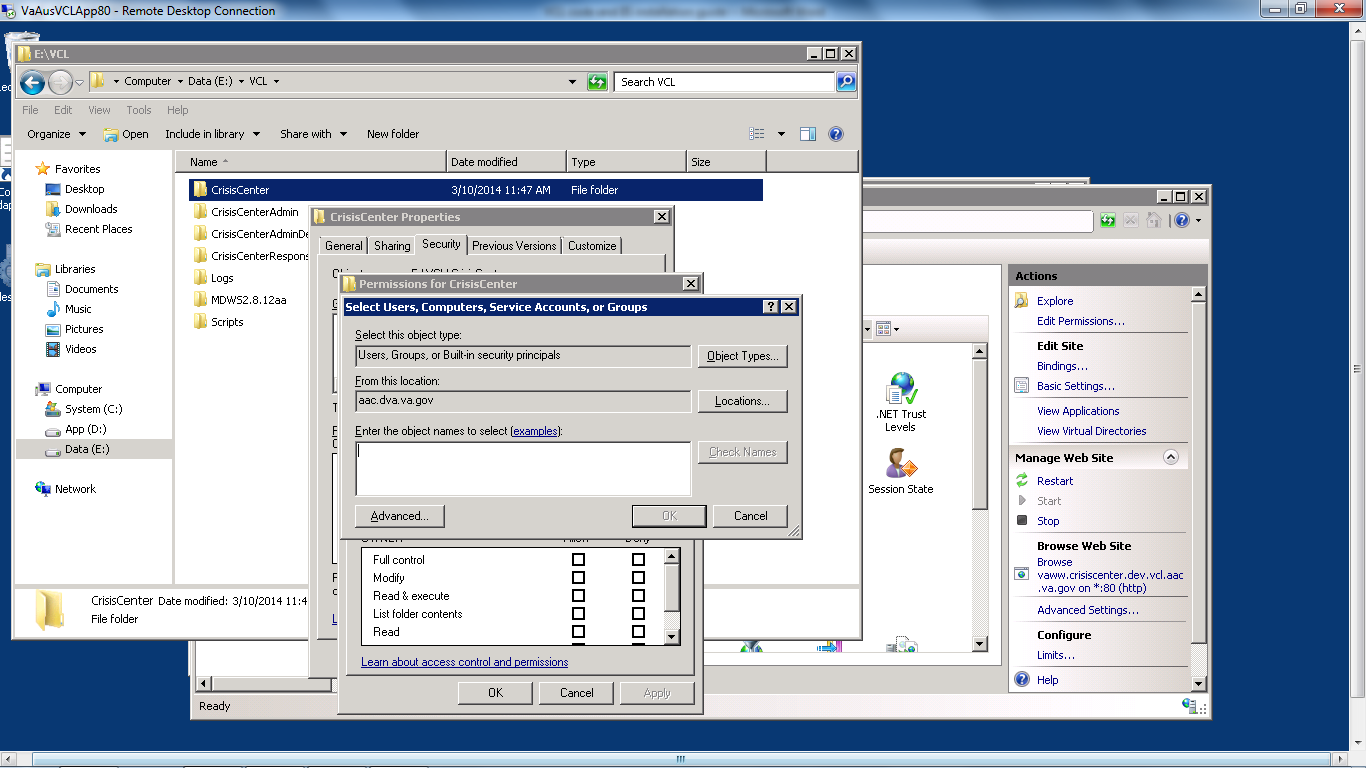


Figure 14: Permissions for CrisisCenter

1. Click Locations, and select the IIS server hosting the VCL code.

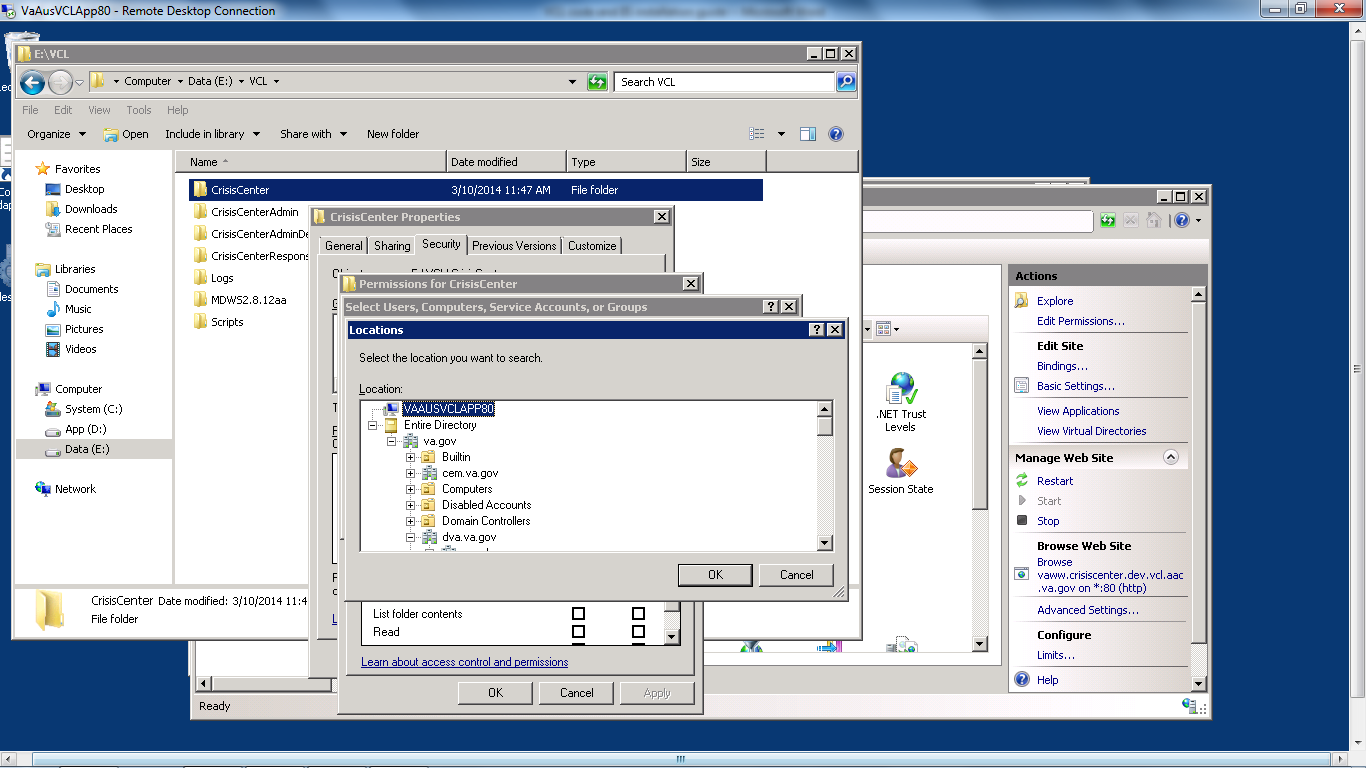


Figure 15: Locations

1. Click OK. Under “Enter the object names to select”, type “IIS APPPOOL\CrisisCenter” for the CrisisCenter website.

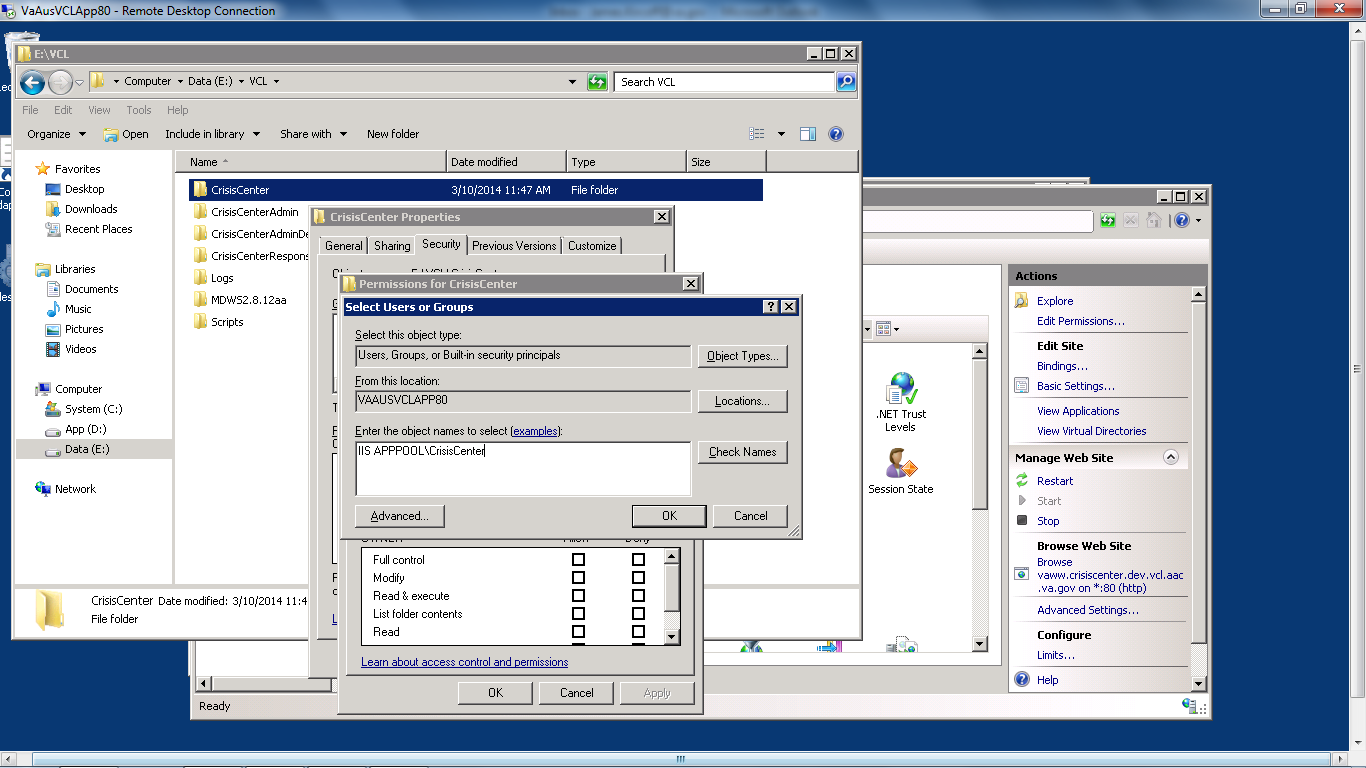


Figure 16: Enter the Object Names to Select

1. Click Check Names to verify your entry was correct. If so the text you entered will change to the name of the appropriate application pool.

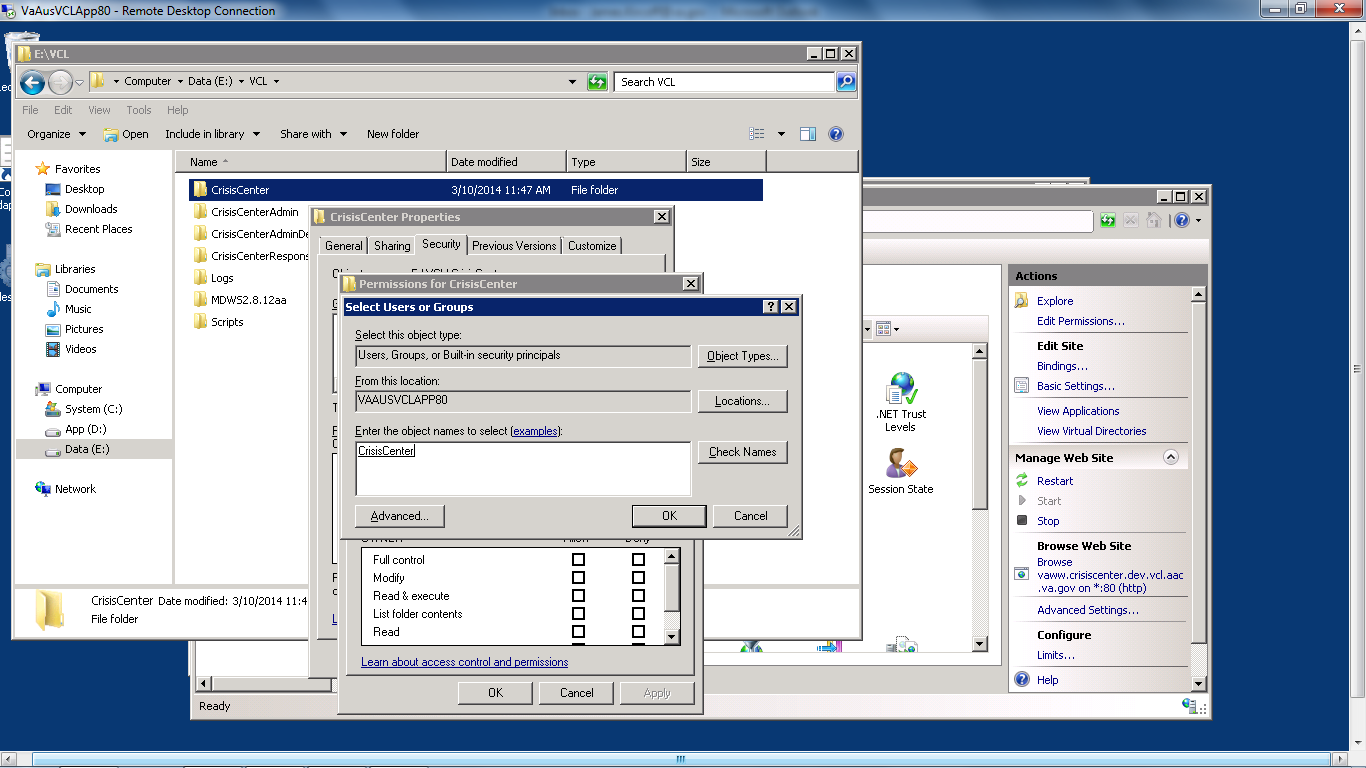


Figure 17: Check Names

1. Click OK. Leave the default permissions granted to the application pool account.

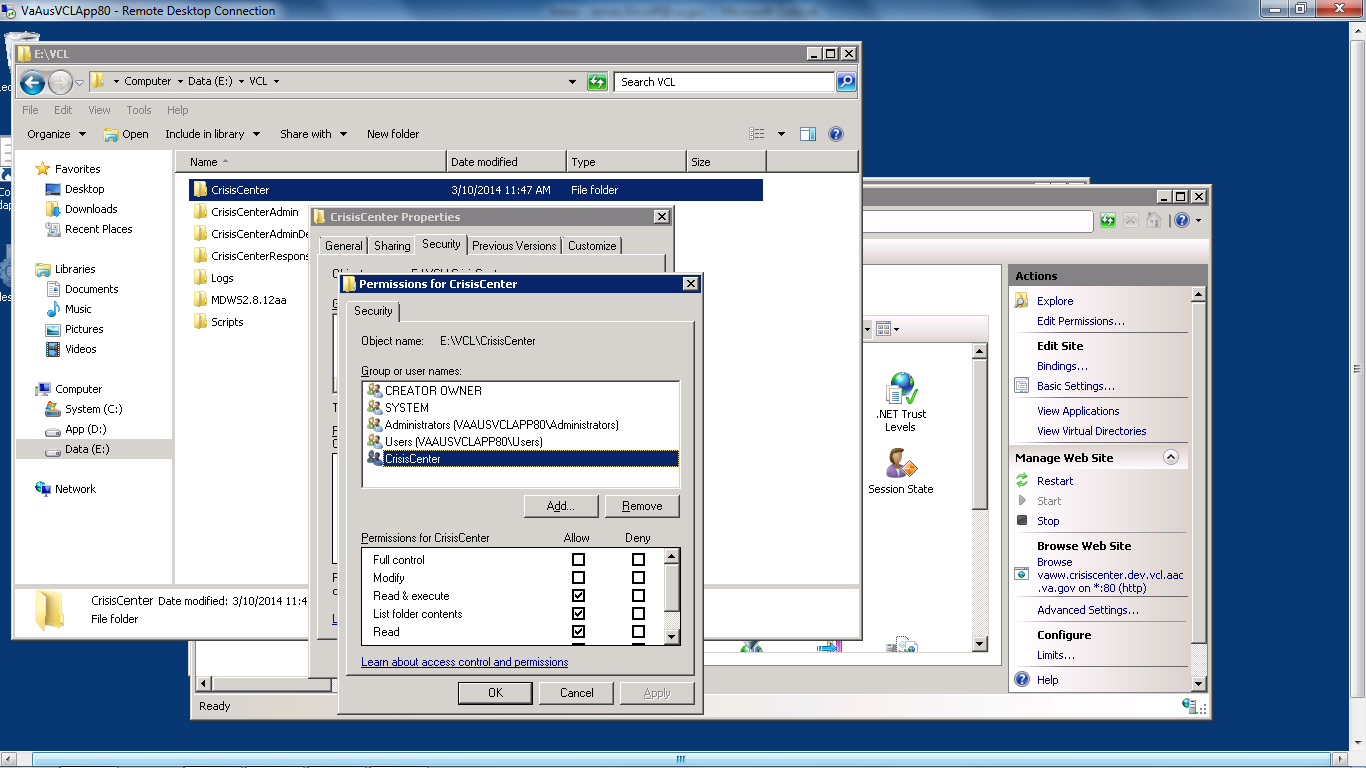


Figure 18: Default Permissions

1. Click OK until all folder property windows are closed.

**Admin application pool permissions**

1. Give the Admin application pool file system permissions to access the Admin code. Open Windows Explorer, navigate to E:\VCL\, right-click the CrisisCenterAdmin folder, select Properties, and select the Security tab.
2. Click the Edit button, then click Add.
3. Click Locations, and select the IIS server hosting the VCL code.
4. Click OK. Under “Enter the object names to select”, type “IIS APPPOOL\Admin” for the Admin website.
5. Click Check Names to verify your entry was correct. If so the text you entered will change to the name of the appropriate application pool.
6. Click OK. Leave the default permissions granted to the application pool account.
7. Click OK until all folder property windows are closed.

**Response application pool permissions**

1. Give the Response application pool file system permissions to access the Response code. Open Windows Explorer, navigate to E:\VCL\, right-click the CrisisCenterResponse folder, select Properties, and select the Security tab.
2. Click the Edit button, then click Add.
3. Click Locations, and select the IIS server hosting the VCL code.
4. Click OK. Under “Enter the object names to select”, type “IIS APPPOOL\Response” for the Response website.
5. Click Check Names to verify your entry was correct. If so the text you entered will change to the name of the appropriate application pool.
6. Click OK. Leave the default permissions granted to the application pool account.
7. Click OK until all folder property windows are closed.

**Web site IIS authentication pass-through settings.**

1. In IIS Manager, select the CrisisCenter virtual directory. Under IIS in the center of the IIS Manager, select Authentication. Under Actions on the right hand side of the IIS Manager, select Basic Settings.

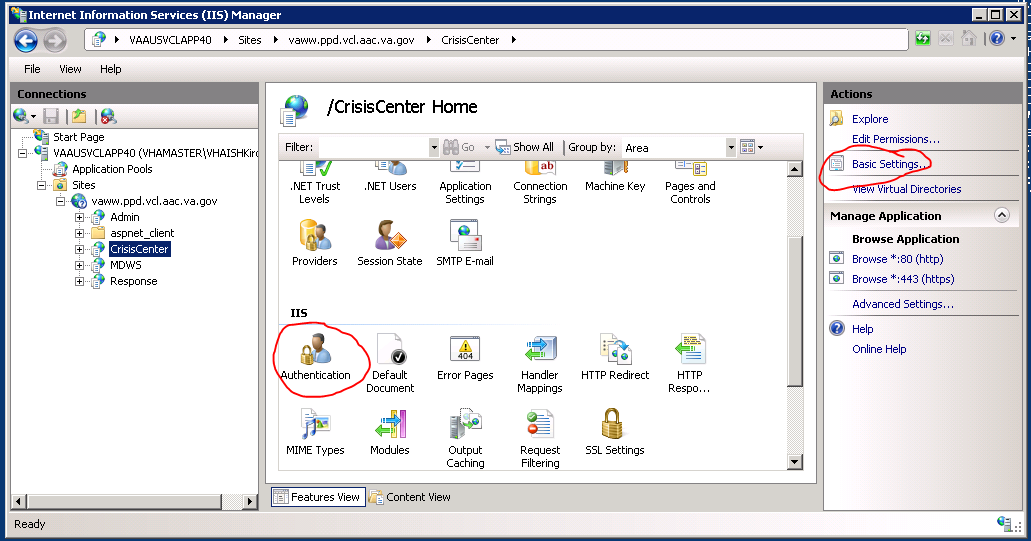


Figure 19: IIS Manager, CrisisCenter Virtual directory

1. Click Connect As.

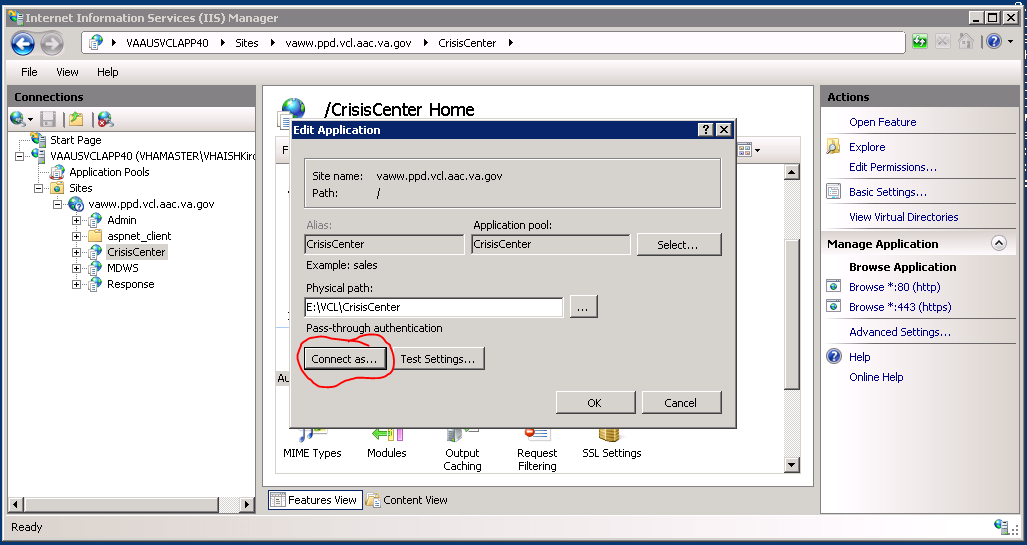


Figure 20: Edit Application

1. Select “Application user (pass-through authentication).

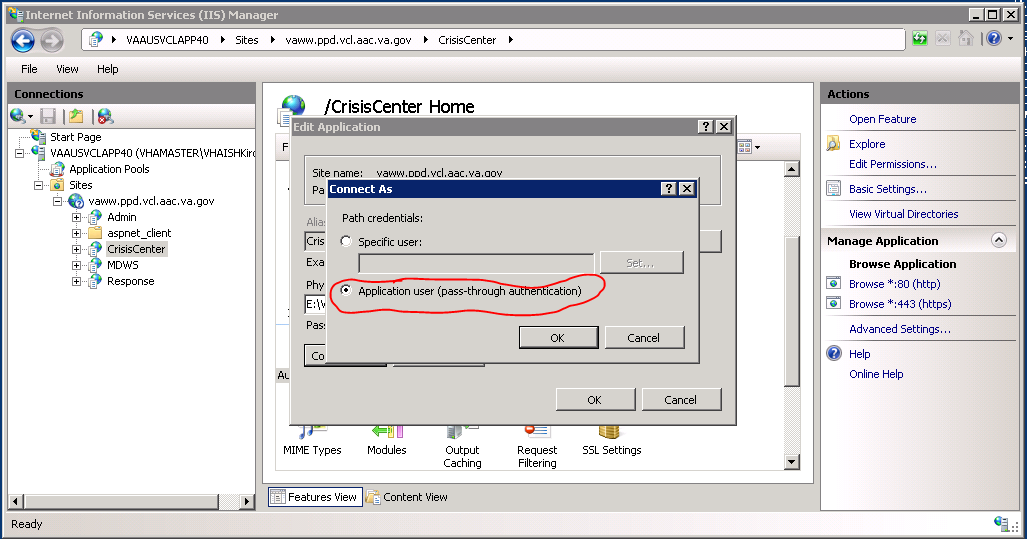


Figure 21: Connect As dialogue

1. Click OK on the “Connect As” window and the “Edit Application”, which will return you to IIS Manager.
2. In IIS Manager, select the Admin virtual directory. Under IIS in the center of the IIS Manager, select Authentication. Under Actions on the right hand side of the IIS Manager, select Basic Settings.
3. Click Connect As.
4. Select “Application user (pass-through authentication).
5. Click OK on the “Connect As” window and the “Edit Application”, which will return you to IIS Manager.
6. In IIS Manager, select the Response virtual directory. Under IIS in the center of the IIS Manager, select Authentication. Under Actions on the right hand side of the IIS Manager, select Basic Settings.
7. Click Connect As.
8. Select “Application user (pass-through authentication).
9. Click OK on the “Connect As” window and the “Edit Application”, which will return you to IIS Manager.

**Session state server set-up**

**Web site set up verification**

***Note****: The following are links for pre-production and production environments:*

Dev  
REDACTED

PreProd/Test

REDACTED

Prod

REDACTED

There are sub-sites in each environment:

For example, vcl.aac.va.gov/admin, vcl.aac.va.gov/crisiscenter, vcl.aac.va.gov/MDWS, and vcl.aac.va.gov/response.

1. Test each site out to see if they work properly. You will get screens like the following if the sites are working:

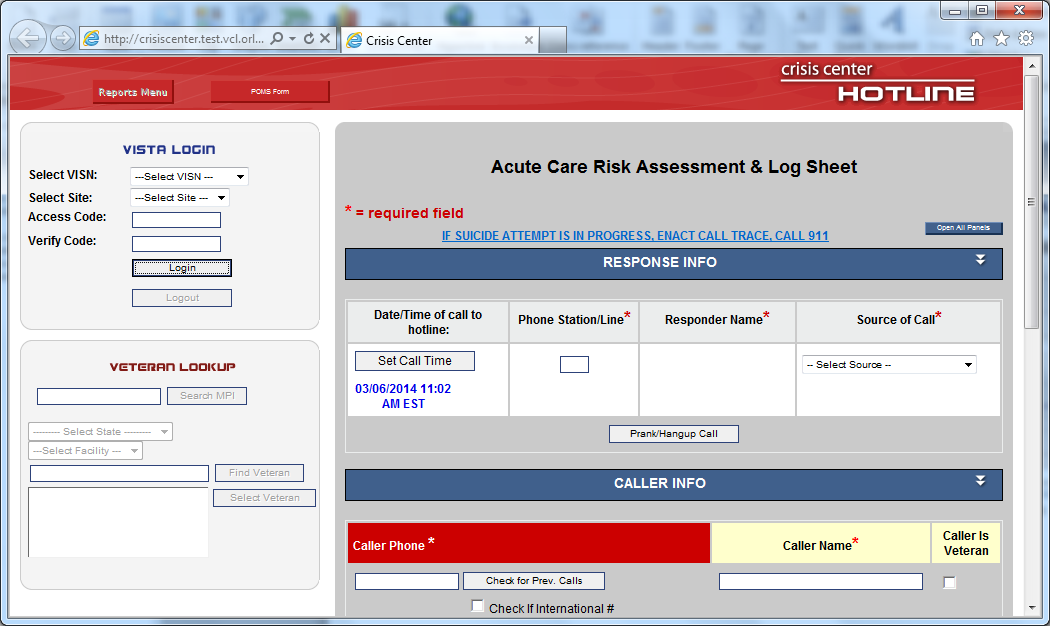


Figure 22: Crisis Center Hotline Login

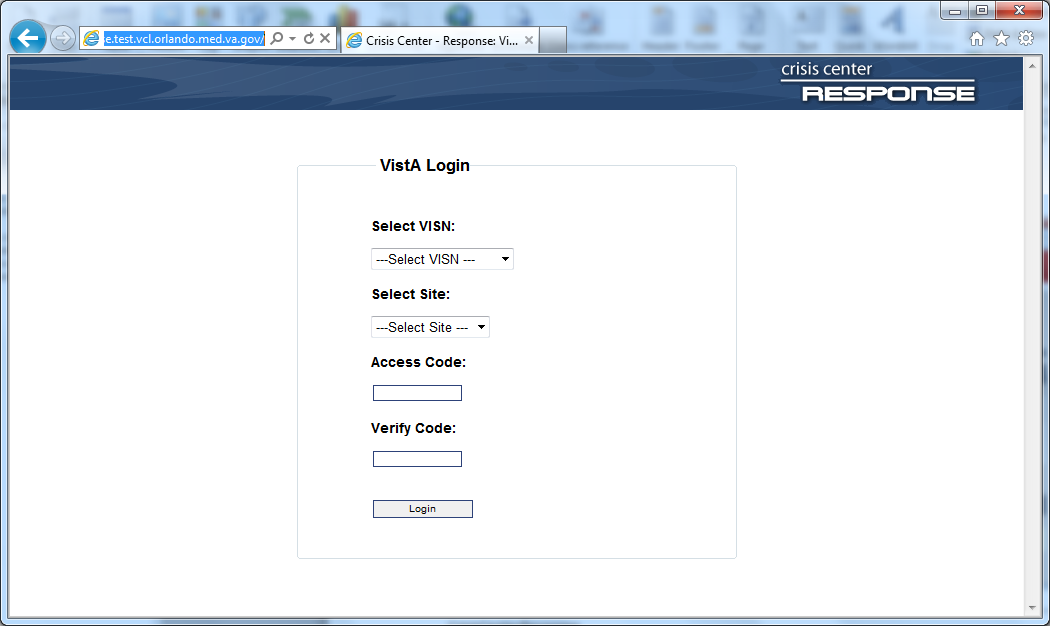


Figure 23: CrisisCenter Response

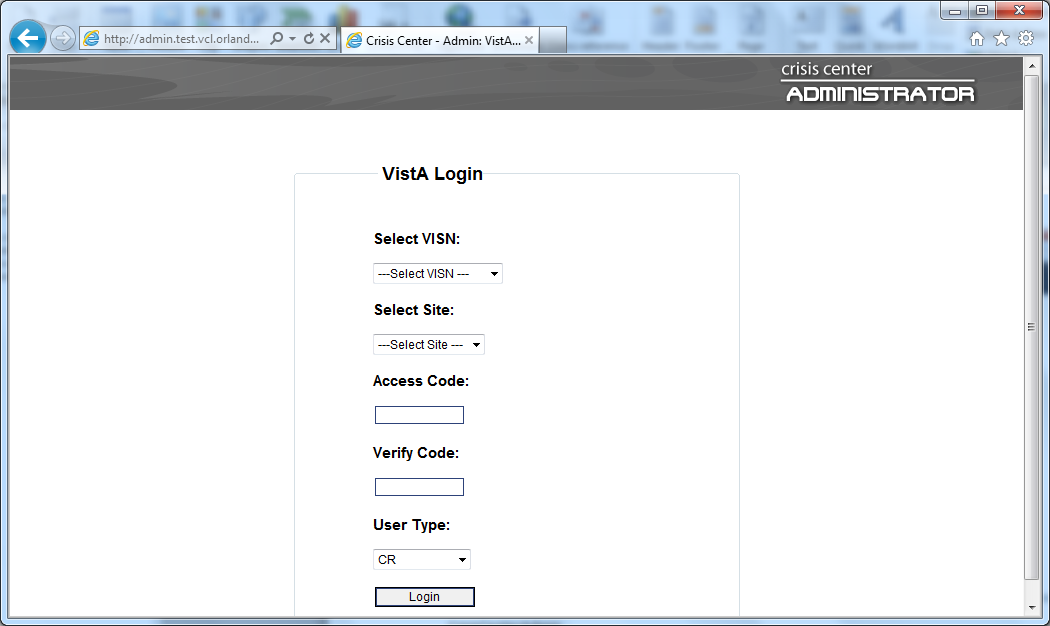


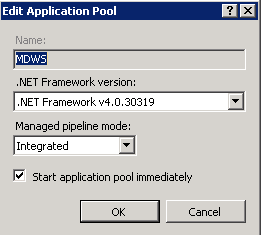
Figure 24: CrisisCenter Administrator

## MDWS installation

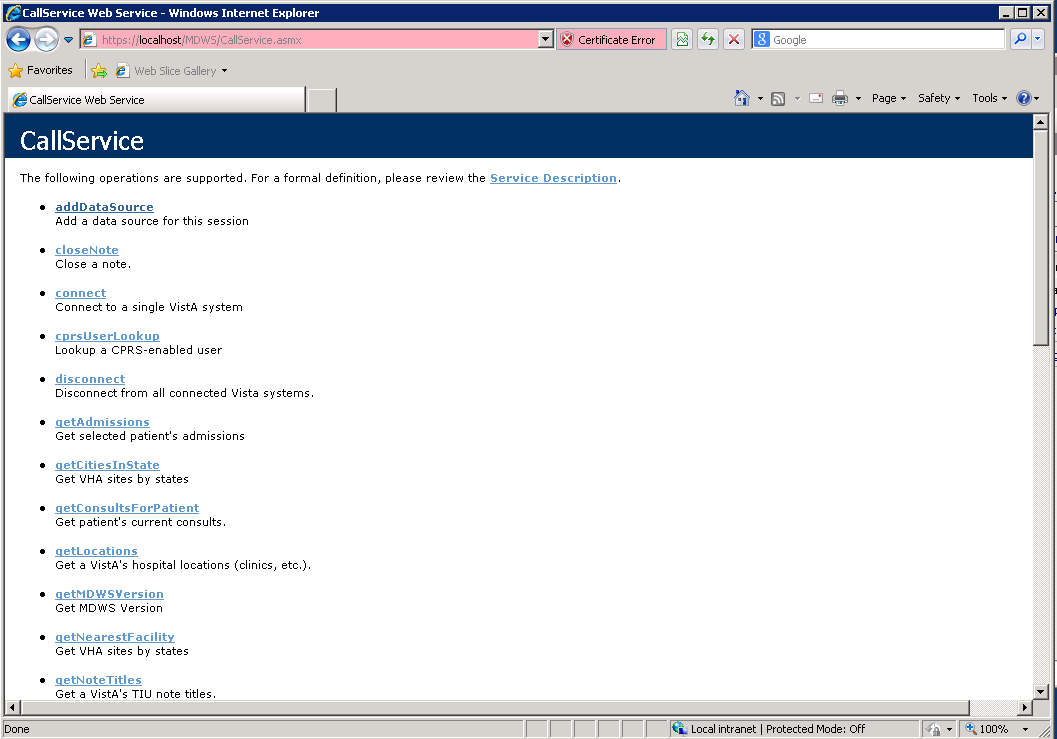
MDWS is the web service application that bridge the gap between VCL applications and VistA sites. Current version used 3.0.3.5. The installation file is provided.

Installation Steps:

1. Verify the .NET Framework 4.0 is installed on the server. If not then install it.
2. Obtain the MDWS files from REDACTED.
3. Extract archive to E:\VCL\MDWS.
4. Open IIS Manager and select Application Pools.
5. Create an application pool with the following parameters:



1. Under Sites, right click the server website name and select Add Application.
2. Fill in the following information for the MDWS web application:
   1. Site name: MDWS
   2. Application pool: MDWS
   3. Physical path: E:\VCL\MDWS
3. Set up the session state server for MDWS by going to the server website/MDWS Home -> ASP.NET, then double-click Session State.
4. Under Session State, select In Process, and then click Apply
5. Give the MDWS application pool file system permissions to access the MDWS code. Open Windows Explorer, navigate to E:\VCL\, right-click the MDWS folder, select Properties, and select the Security tab.
6. Click the Edit button, then click Add.
7. Click Locations, and select the IIS server hosting the MDWS code.
8. Click OK. Under “Enter the object names to select”, type “IIS APPPOOL\MDWS” for the MDWS website.
9. Click Check Names to verify your entry was correct. If so the text you entered will change to the name of the appropriate application pool.
10. Click OK. Leave the default permissions granted to the application pool account.
11. Click OK until all folder property windows are closed.
12. Once completed, test it going to https://localhost/MDWS/CallService.asmx in a browser on the server.



**Obtaining the VCL Installation Files**

* The VCL application code will be provided in a ZIP archive. This archive is to be unpacked in the directory that will host the three websites needed for VCL: Hotline, Response, and Admin. The lead developer of the VCL team will have the location of the archive of the code files. These files will be uploaded into vaausvclapp80\vcl into a file name that includes software version information
* The VCL database installation is performed by restoring from a SQL Server backup file. The details regarding file name and location should be available with the Database Administrator. (Dev and PPD data exports will be uploaded into vaausvclapp80\vcl. PRD data transfer will be accomplished according to the separate Data Transfer Agreement.)

Perform a restore for the VCL database, using the appropriate backup file. A sample restore statement is provided below:

RESTORE DATABASE [NationalSuicideHotline\_PreProd] FROM

DISK = N'C:\0\_VCL\TEMPDB-Backup'

WITH FILE = 1,

MOVE N'NationalSuicideHotline' TO N'C:\0\_VCL\PreProd\NationalSuicideHotline\_PreProd\_dat.mdf',

MOVE N'NationalSuicideHotline\_log' TO N'C:\0\_VCL\PreProd\NationalSuicideHotline\_PreProd\_log.ldf',

NOUNLOAD,

STATS = 10

GO

## System Requirements

Storage requirements for installation:

|  |  |
| --- | --- |
| **Type of Data** | **Size** |
| Applications | < 5MB |
| Help Files | < 1MB |

Sites should reserve 1KB of storage space per observation for data that will accumulate. The vast majority of growth will occur in the OBS file (#704.117).

The following describes the installation environment for on the VistA client workstation:

* Workstations must be running under Windows. Refer to <http://vaww.vairm.vaco.va.gov/vadesktop> for additional information on VA standard desktop configurations.
* Remote Procedure Call (RPC) Broker Workstation must be installed.
* The workstation must be connected to the local area network.
* Administrator privileges are needed on any machine on which CP Gateway Service is installed.

# Backout Plan

This section outlines the back out procedures for VCL.

During installation of a new VCL baseline, if there are any issues with new baseline, the new baseline will be backed out and the system will be restored to the previous baseline.

In the event that a backout of the VCL installed code is needed, code should be rolled back to the last known working version. AITC will retrieve the tape backup of the last known good production version to reinstall. The database admin and system admin will determine the correct last working version to rollback to.

The following are the steps to back out VCL to its previous version:

1. Notify the **Remedy Help Desk** REDACTED and VCL application users about backout plan initiation.
2. When VCL is first deployed to AITC, a copy of the existing VCL install files will be placed at **vaausvclapp80\vcl**.
3. Disable user access to the VCL system while the back out procedures are in process.
4. Delete all of the VCL code from the following location where it was uploaded onto the dev server:

vaausvclapp80\vcl\vcl-2.0 build 21.zip (Build information is provided as an example.) The VCL code will be in an archive, with a naming convention that identifies the version, and when unpacked will have a directory structure similar to the following:

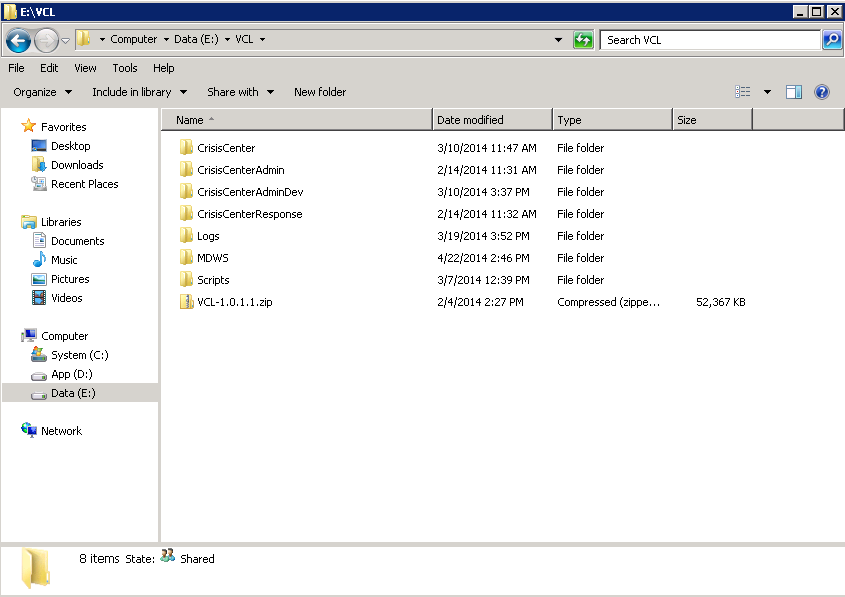


Figure 25: Unpack VCL Code Archive

1. Rename the backup copied folders. Backup the VCL database on the dev server (**vaaussql1a**.)
2. Perform a full database backup of database "**NationalSuicideHotline\_Test**" on **vaaussql1a**.
3. Create an additional backup VCL folder at an additional location on **vaaussql1a** in case the VCL application needs to be backed out again.
4. Conduct system health checks of the VCL application.
5. Enable VCL application user access.
6. Notify the **Remedy Help Desk** (1-888-596-4357) and VCL users of successful backout.

# Post Installation Instructions

The AITC Build Manager will submit the needed access request forms (if not already submitted) for the environment. Where possible, a primary POC for each group of permissions being granted will be designated. The System and Database Administrators will complete the SDM tasks needed to grant access as required. The primary POC for each group should be contacted to verify access.

***Note:*** *This Install Guide Addresses the basic "vanilla" product.*

After completing the instructions contained in this Guide, please apply the Patch in order to upgrade the product to the latest version. We need to include the all the Increment 3 upgrades.

Instructions for the Patch, along with the step-by-step database scripts, have been detailed in change order CO217347FY14.

# Installing and Configuring the SQL Server Reports Server (SSRS) Component

This section is intended to provide a complete step-by-step walkthrough for installing and configuring the SQL Server Reports Server component, for the Veterans Crisis Line application.

## Audience

The intended audience is the System and Database Administrators, and the VCL Manager at AITC.

## Pre-Requisites

The following pre-requisites must be in place before all the steps outlined in this document can be completed:

1. Two security groups will need to be setup in the VA Active Directory:
   * VCL REPORTVIEWER and VCL REPORTMANAGER.

The Group creation process is as follows:

* + First create the Group in the VA active directory
  + Next create a ***database login*** for the Group, in the NationalSuicideHotline database
  + Then create a ***user*** corresponding to the ***login***, in the ReportServerDatabase.
  + Finally, add the authorized individuals, as members of the group.
  + **Notes**:

1. The suffixes \_DEV and \_PPD must be added to these groups, in order to set them up for the Development and Preproduction environments respectively.
2. Group membership is controlled through the AITC user creation process. A “VA 9957” security form must be processed for each member who is added to the group.
3. A “service account” will need to be setup for each environment:

(For the DEV, Pre-Prod and Prod databases, respectively)

1. Dev
   * + 1. VaAacVclAppDev - Development Application Service Account
       2. VaAacVclRptRODev - Development Reporting Service Account
2. Preproduction
   * + 1. VaAacVclAppPpd - PreProduction Application Service Account
       2. VaAacVclRptROPpd - PreProduction Reporting Service Account
3. Production
   * + 1. VaAacVclAppPrd - Production Application Service Account

VaAacVclRptROPrd - Production Reporting Service Account

The service account creation process is as follows:

* + First create the account in the VA active directory
  + Next create a ***database login*** in the NationalSuicideHotline database
  + Then create a ***user*** corresponding to the login, in the ReportServerDatabase.
  + **Note:** This account must have read-only access to all the tables in the VCL Database, EXCEPT for: HotlineCalls, HotlineCalls\_H, HotlineCallsDetails, HotlineCallsDetails\_H.

## Configuring the Reports Server (Includes SSL)

1. From the Start Menu, select “run as Administrator” for the Reporting Services Configuration Manager.

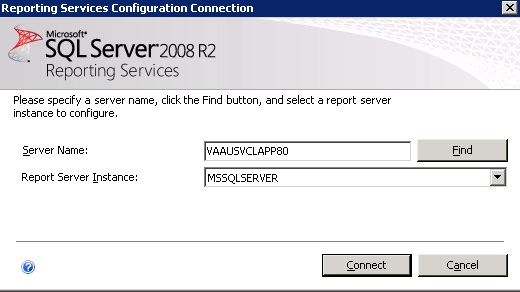


Figure 26: Reporting Services Configuration Connection

Here are the steps to configure SSL on SSRS:

Log on to VCL APP server 🡪 go to Reporting services configuration Manager, see below:

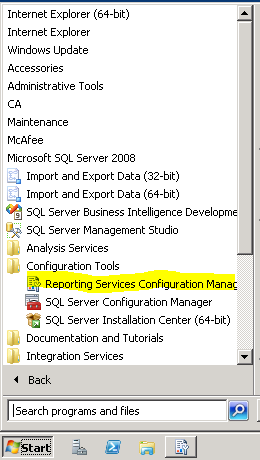


Figure 27: Reporting Services Configuration Manager

Click 🡪 window popup as below:

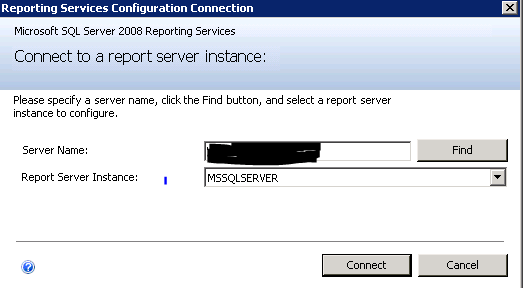


Figure 28: Specify a Server Name

Click Connect 🡪 see the above figure.

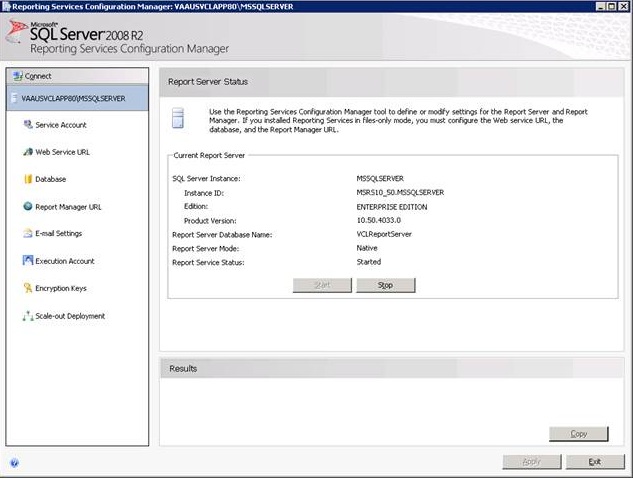


Figure 29: Report Server Status

Select Web services URL from the left-hand pane. Add the SSL certificate and SSL port (see drop-down highlighted in yellow.)

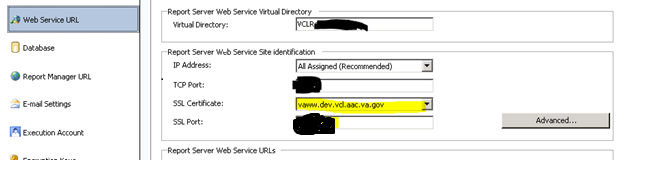


Figure 30: SSL Certificate and SSL Port

Click Advanced and add the following SSL Certificate information (highlighted in yellow below:)

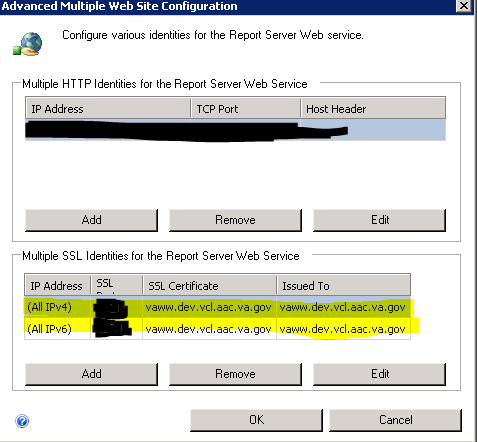


Figure 31: SSL Certification Information

Select the Report Manager URL

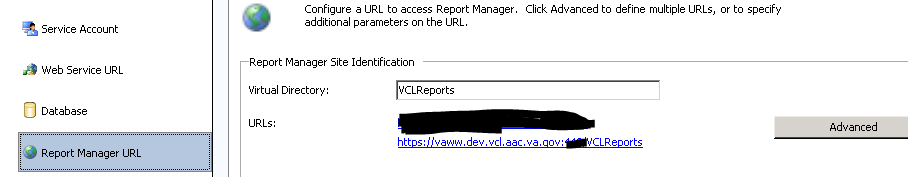


Figure 32: Add Report Manager URL

Click Advanced and add as shown below:

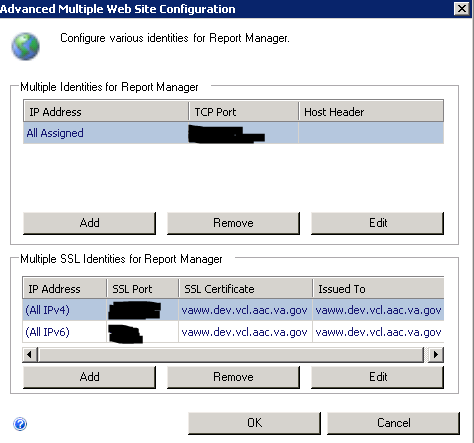


Figure 33: UpdatingSSL Certificates

Click OK.

This will complete the SSL section of SSRS.

## Defining the Reporting Web Project

On the Application server machine (APP80 in case of Dev) open Internet Explorer and go to the reporting services URL.

1. From the Reports Manager home page, create a ***Datasource*** named VCLDatasource.

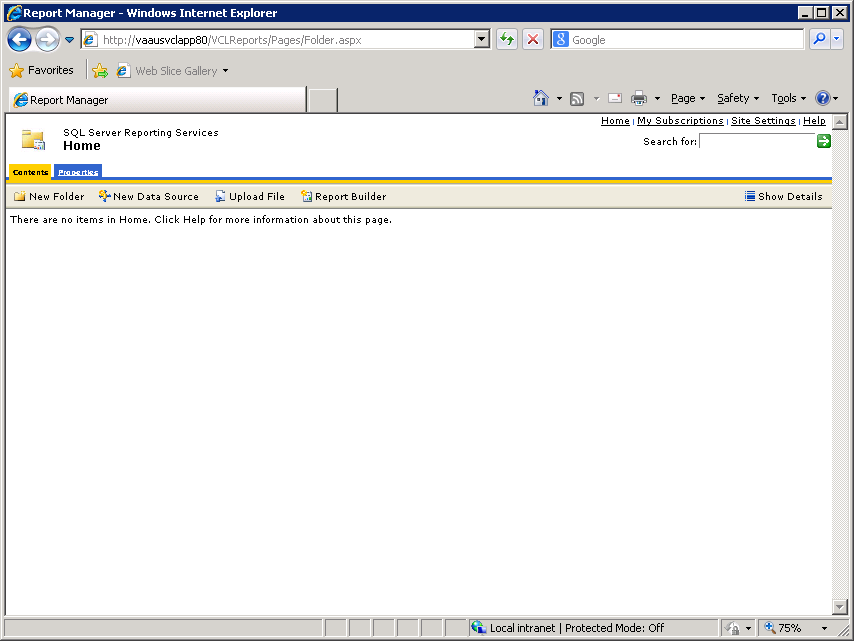


Figure 34: Create a Datasource

1. Select “Credentials stored securely in Reports Server”.

Also check “Use as Windows Credentials when connecting…”

Note: AITC will need to type in the username and password for the service account in this section.

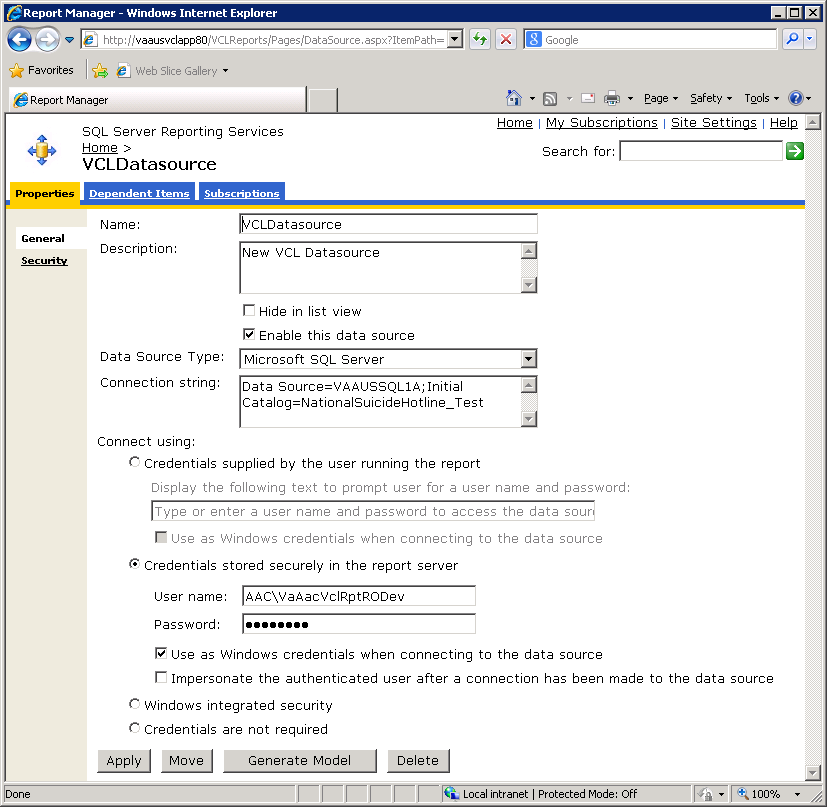


Figure 35: VCL Datasource

1. After the Datasource has been created, select it by clicking on it.
2. Click on Generate Model

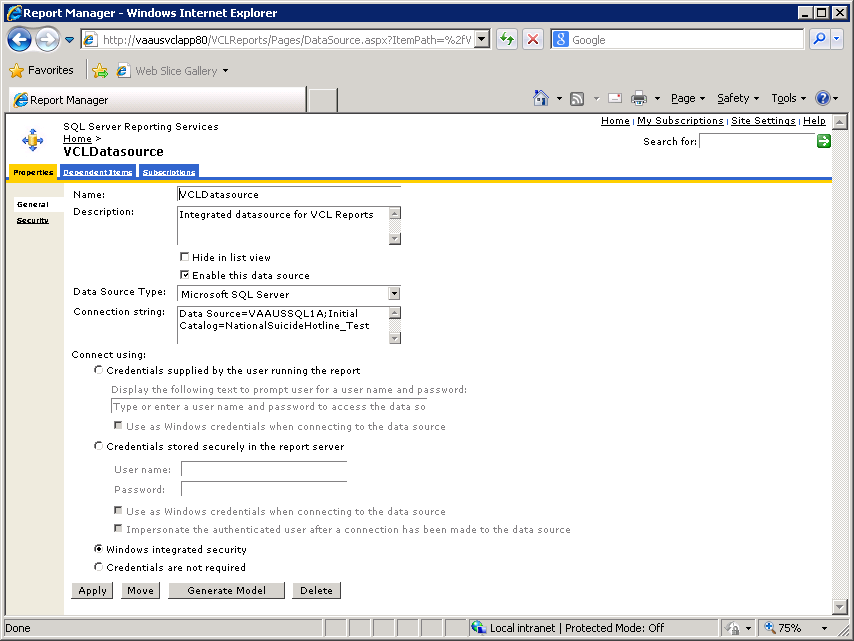


Figure 36: Generate Model

1. Create a new ***Model*** named VCLModel.

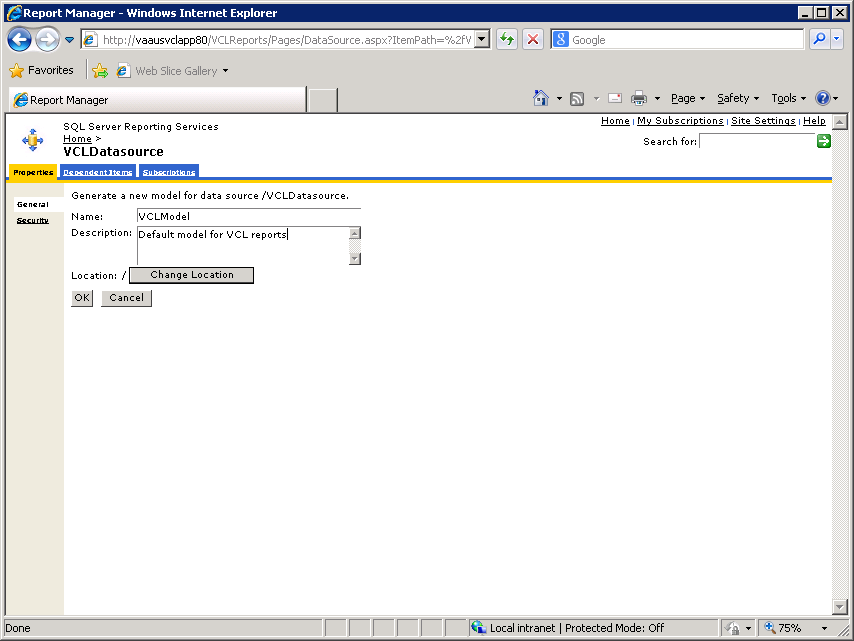


Figure 37: VCL Model

You must define the security, by adding role assignments and giving permissions.

1. To define the security, click on Site Settings.
2. Click New Role Assignment.
3. Add VCLREPORTMANAGER, as “System User” (allows Manager to see Report Builder link).

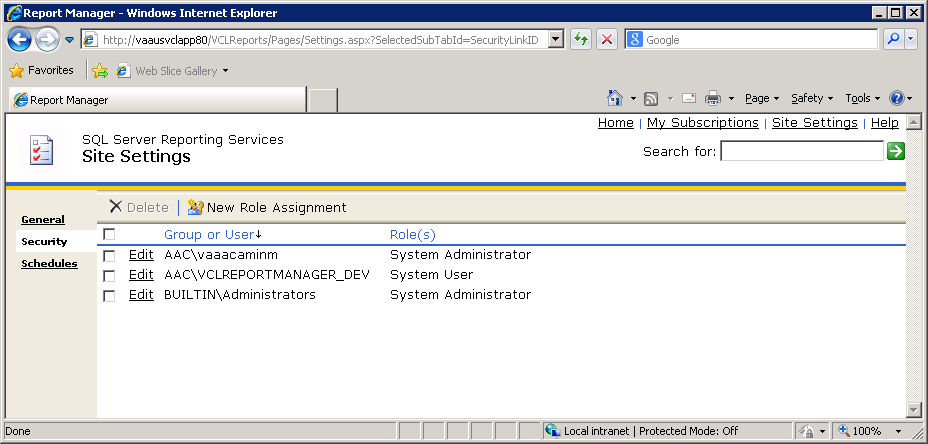


Figure 38: System User

Next, define the security for all the items that will be created.

1. Click the Home link, then Properties tab.
2. Click on ***New Role Assignment***, add VCLReportManager and VCLReportViewer.

Manager gets Browser, Publisher and ReportsBuilder permissions. The Viewer group gets only Browser and Builder permissions.

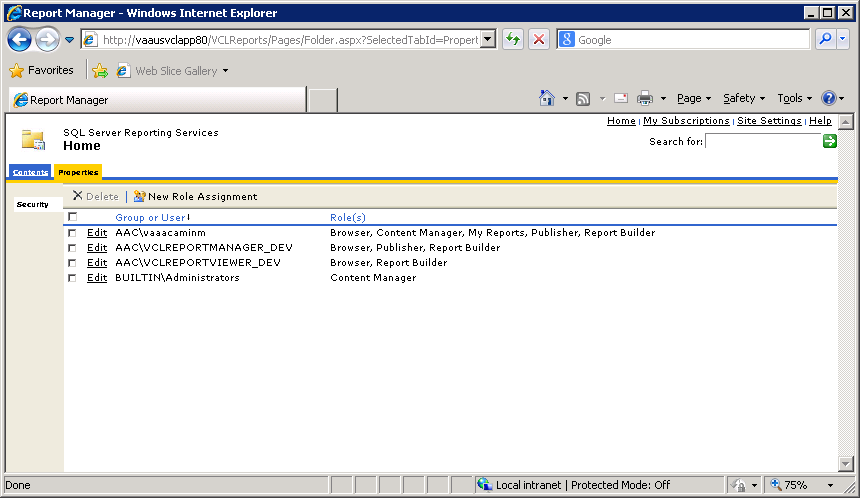


Figure 39: New Role Assignment

Next, ensure that the Datasource cannot be modified by anyone.

1. Click on the Datasource, and select the Security tab.
2. Ensure that even the MANAGER role can only see (but not alter) this particular object.

This is called Item-level security.

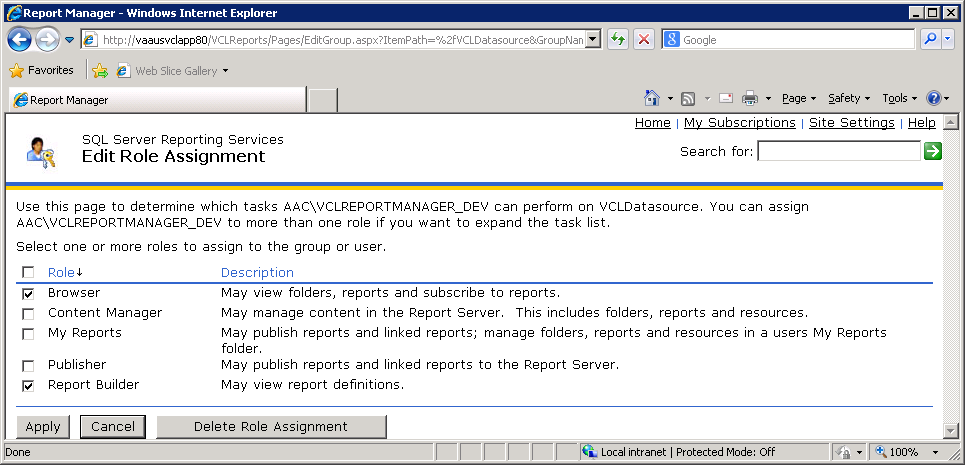


Figure 40: Edit Role Assignment

Similarly, you will want to override the inherited security for this item and set Item-level security for the Model as well:

1. Click on the Model, and select the Security tab.
2. Ensure that even the MANAGER role can only see (but not alter).

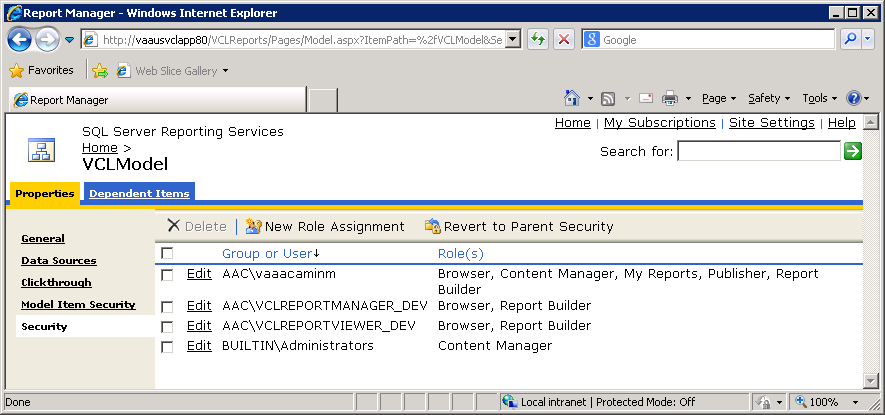


Figure 41: Security

1. Also, check the “Hide in List View” flag for the model. This will prevent its accidental deletion by the end user.

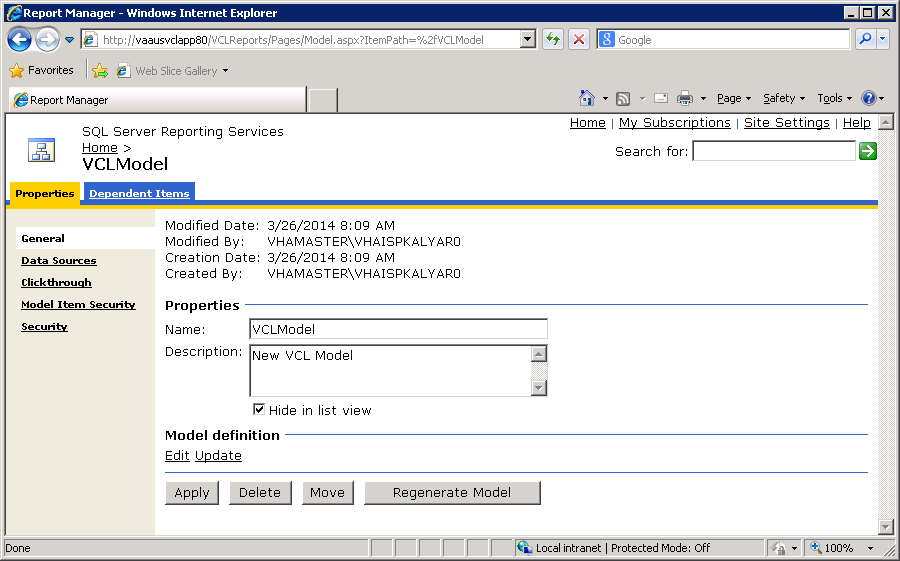


Figure 42: Properties

### Customizing the Site name:

Click on Site Settings, then General. Enter the following text: Veterans Crisis Line – Custom Reports.

**Note:** Append (DEV) or (TEST) for those environments respectively.

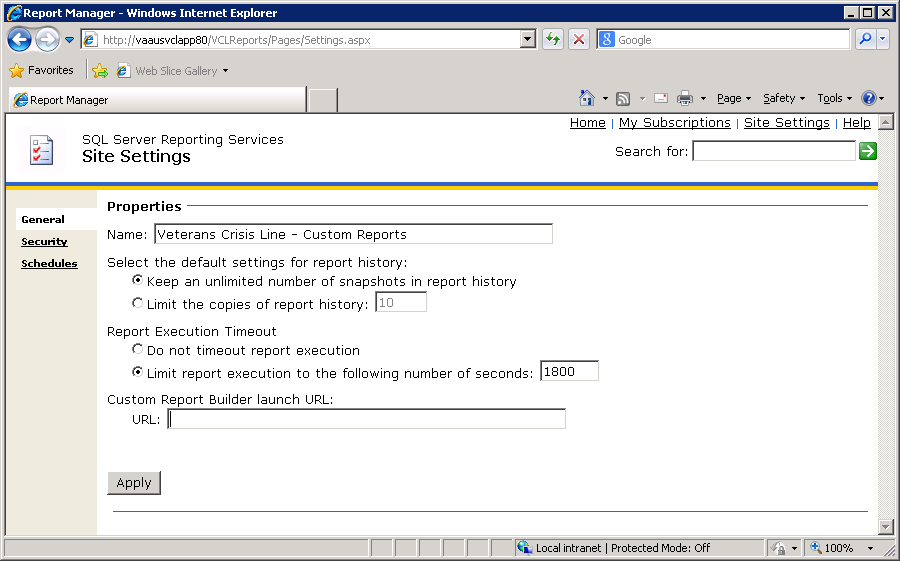


Figure 43: Veterans Crisis Line – Custom Reports

|  |  |
| --- | --- |
|  |  |

## Reporting Services SSL Configuration

This has been covered in section 6.3

## Uploading Previously Developed “Sample Reports” to the Server

|  |  |
| --- | --- |
| **On the Application server machine (APP80 in case of Dev) open Internet Explorer and go to the reporting services URL.** | |
| 1. | The pre-defined reports are located in the following folder on VaAusVclApp80 (the Dev Application Server):  E:\VCL\Scripts\Report\_scripts  At the Reports Manager home page, select ***Upload File*** and upload the .rdl report files one by one. |

Figure 44: Upload File

# Patching the Production Environment with Updated Code

In the event that a patch needs to be installed in the AITC production environment, the following steps should be followed.

1. Copy the patch files REDACTED
2. Write documentation that details how to install the patch. Use the following steps as a guideline. You may need to revise to meet your local environment specifications.

* Open IIS Manager, expand Sites, and select the vaww.vcl.aac.va.gov website.
* Under Manage Web Site, click Stop.
* Copy code base archive REDACTED to production environment, and unzip.
  + - Copy all files and folders from CrisisCenter to E:\VCL\CrisisCenter, overwriting existing files and folders.
    - Copy all files and folders from CrisisCenterAdmin to E:\VCL\CrisisCenterAdmin, overwriting existing files and folders.
    - Copy all files and folders from CrisisCenterResponse to E:\VCL\CrisisCenterResponse, overwriting existing files and folders.
* Return to IIS Manager and click Application Pools.
* Select the CrisisCenter application pool.
* Under Application Pool Tasks, click Recycle.
* Select the CrisisCenterAdmin application pool.
* Under Application Pool Tasks, click Recycle.
* Select the CrisisCenterResponse application pool.
* Under Application Pool Tasks, click Recycle.
* Under Sites, select vaww.vcl.aac.va.gov website.
* Under Manage Web Site, click Start.

1. Send an email to the AITC team requesting a Change Order (CO) be opened for a patch be installed, and attach the installation instructions to the email. REDACTED For example:

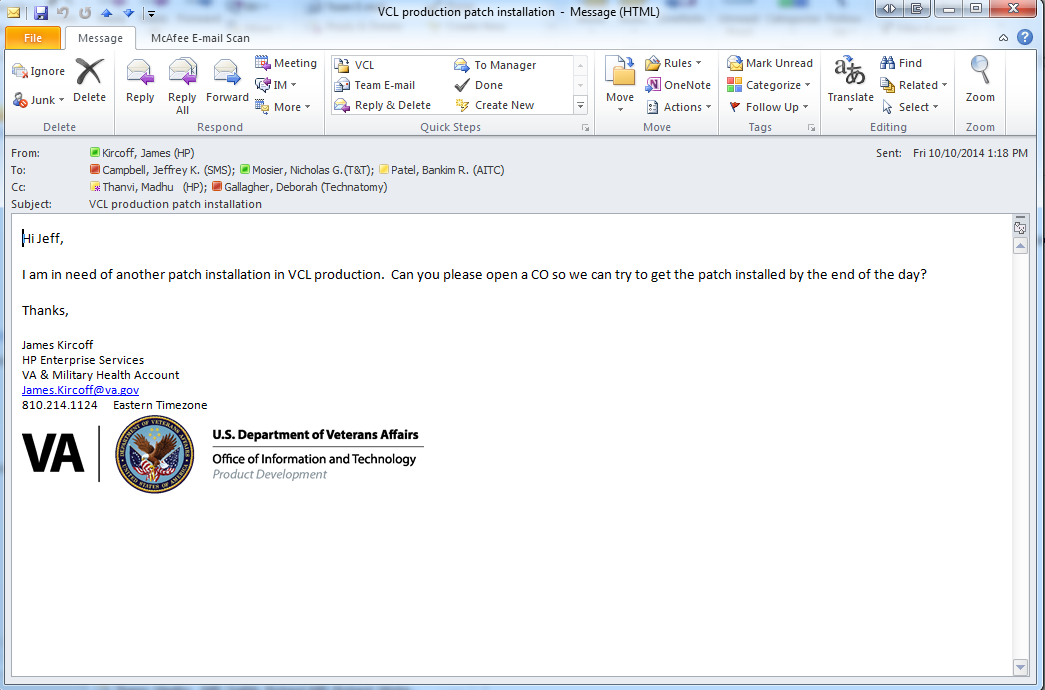


Figure 45: Change Order Request Email

1. Wait for the AITC team to respond back saying they have installed the patch.
2. Verify your patch was installed successfully. If required, have a VCL user log in and verify it for you.

# Troubleshooting

VCL development team participated with AITC resources during a dry run of the install process and any problems encountered were remediated and incorporated into this guide. VCL developers are available during the installation for assistance.

## Rollback Instructions

For initial release, if there are any issues with the first migration, the rollback plan is to revert back to the Orlando environment.

After initial release, if there are any issues with the VCL application, the necessary action is to roll back to the last clean working version. The database admin and system admin should determine the correct last working version to rollback to.

The following are the steps to return the VCL database to its last working version:

1. Restore database "**NationalSuicideHotline\_Test**" from the backup version from step 7 of the above Backout Procedures.

The database restore will clean the database and restore it to the clean state created in step 7 of Section 3.5.3 Backout Procedures.

1. Confirm that the backup and new working application folders are renamed.
2. Test the VCL application and confirm that the restored version is working correctly.

Refer to section 6.6 of the [ISCP](http://vaww.oed.portal.va.gov/projects/vet_crisis_line_enhancements/Library/Forms/AllItems.aspx?RootFolder=%2fprojects%2fvet%5fcrisis%5fline%5fenhancements%2fLibrary%2fUser%20Documentation%20and%20National%20Release&FolderCTID=0x012000836A27F944BCDA4390DB2BFA889E1A7E&View=%7bC98F591B%2d0DD2%2d41E1%2d9CA2%2d2807E05B1B74%7d) for key contacts in the event that a rollback for the VCL software is needed.

# FAQ

|  |  |
| --- | --- |
| **Question** | **What do I do if I have installation issues?** |
| **Response** | 1. If assistance is needed during installation, please create a Remedy Ticket or contact the REDACTED |
| **Question** | **How can I check my connection to the broker server?** |
| **Response** | 1. Check the windows registry (HKLM/software/vista/broker/servers) key and ensure that the key is set to the correct IP and port. 2. Check that the broker is running on the correct instance of VistA and on the correct port.   Type D ^%SS to show the list  Find the instance and find the line XWBTCPL  Verify that the TCP|port number is correct |
| **Question** | **How can I check the Windows application Event Notifier?** |
| **Response** | 1. Right-click **My Computer**. 2. Select **Manage**. 3. Expand **Event Viewer**. 4. Select **Application**. |
| **Question** | **How do I stop the CP Gateway Service?** |
| **Response** | 1. In Windows, click **Start** | **Control Panel** | **Administrative Tools** | **Services**. The Services window displays. 2. Click the Clinical Procedures Gateway row. A link, Stop the service, displays. 3. Click **Stop**. A progress window displays as the service stops. 4. When the progress window closes, the Services window redisplays. The status column in the Clinical Procedures Gateway row displays **Stopped**. |
| **Question** | **How can I change the time interval for CP Console and CP Flowsheets at which they time out?** |
| **Answer** | The time interval is set using the TIMED READ value in the NEW PERSON file (#200). |
| **Question** | **What are the post-deployment requirements for testing the successful install?** |
| **Answer** | * Verify the code deployment * Validate connections with other systems |