Department of Veterans Affairs

Mental Health eScreening System

San Diego Implementation Plan

July 2015

Software Version 1.0

Revision History

Date	Version	Description	Author
July 2015	1.6	Updated the server memory description	Information Innovators Inc.
July 2015	1.5	Simplified the setup process	Information Innovators Inc.
June 2015	1.4	Additional VA revisions	Laine Deighan
April 2015	1.3	Revised per VA	Laine Deighan
February 2015	1.2	Final document	Laine Deighan
October 2014	1.1	Revised draft	Laine Buckwalter
February 2014	1.0	Draft	Mike Roberts

Contents

1.0 INTRODUCTION 1

1.1 Research Pilot Findings of MHE Benefits 1
1.2 Purpose 2
1.3 Project Oversight 2
1.4 System Overview 2
1.5 Scope 4
1.6 Stakeholder Approach 4

2.0 ASSUMPTIONS 4

2.1 Technical 4
2.2 Organizational 5

3.0 ROLES AND RESPONSIBILITIES 5

3.1 Implementation Team Information 5
3.2 Points of Contact 6
3.3 San Diego Key Positions 6
3.4 Coordination 7
3.5 Site Notification of Product Release 7

4.0 OVERALL SPECIFICATIONS 7

4.1 Rollout 7
4.2 Defect and Bug Support 7
4.3 Training 8
4.4 508 Compliance 8
4.5 User Acceptance Testing 8
4.5.1 Preparation 8
4.5.2 Deployment 8
4.5.3 VA UAT 9
4.5.4 Post-UAT Issue Resolution 9

5.0 TRANSITIONING PILOT TO BE RUN 100% BY VA IT AND CLINICAL STAFF 10

5.1 Transition Overview 10
5.2 Maintenance 10
5.2.1 Routine Maintenance 10
5.2.2 Database backups 10
5.2.3 Operating system updates 10
5.2.4 System recovery procedures 11
5.2.5 Application configuration 11
5.2.6 Application or database code changes 11
5.3 Software 11
5.3.1 Server Software 11
5.4 eScreening production deployment information 12
5.5 Creating a new eScreening instance 12
5.5.1 Creating the Instance Tomcat Base Directory 12
5.5.2 Installing Instance IIS Service 12
5.5.3 Adding Instance IIS Proxy Rule 13
5.5.4 Creating an Instance Database 14
5.5.5 Creating an Instance Deployment Staging Area 15
5.5.6 Restarting Tomcat 15

5.5.7 Supporting Software 15
5.5.8 Firewall 16
5.5.9 Client Software 16
5.5.10 VPN Software 16
5.5.11 Operating System 17
5.5 Hardware Physical Description 17
5.6 VistA Resources 18
5.6.1 VistA Proxy Account 19
5.6.2 SSL Certificate 20
5.7 Network Resources 20
5.7.1 Firewall 20
5.7.2 DNS 20
5.7.3 VPN 20
5.8 Facilities 20
5.9 Tablet Management 21
5.9.1 Sanitation 21
5.9.2 Inventory 21
5.9.3 Missing tablets 22
5.9.4 Disposal 22
5.9.5 Samsung Tablet Security Steps 23
5.10 Personnel 23

6.0 IMPLEMENTATION TASKS AND ACTIVITIES 24

6.1 Operations and Support 24
6.1.1 OIF/OEF/OND Care Management 24
6.1.2 Primary Care 25
6.1.3 Mental Health Access Clinic 26
6.2 Entering and Editing Assessments by VA professional staff (Customizing MHE for your clinic) 26
6.2.1 Batteries (Assessments) 27
6.2.2 Modules 28
6.2.3 Sections 29
6.2.4 Rules 29
6.3 Outreach scenarios 30
6.4 Transferring tablets to a different facility 30
6.5 Training 30
6.6 Activation 30
6.7 Support 30

7.0 TRANSITIONING TO REMOTE ASSESSMENTS (FROM STANDARD PRACTICE TO USING MHE) 31

7.1 Planning the Transition 31
7.2 Best Practices Suggestions 31

8.0 RISKS AND MITIGATIONS 32

APPENDIX A – OIS RISK BASED DECISION MEMO 33

APPENDIX B – VA OI&T MOBILE DEVICE MANAGEMENT 37

APPENDIX C - MHE SAMSUNG TABLET SECURITY STEPS 41

1) Change the View for the Assessment 43
2) Download Keycall off of R Drive 43
3) Add Printer to the Tablet 43

4) Authorizing VHASDCESCREEN to Have Administrator's Rights 43
5) Prevent Microsoft Lync from Launching at Startup. 43
6) Install Mozilla Firefox 29.0 43
7) Disable Access to IE 44
8) Unpinning All Icons (Except Firefox) on the Task bar 44
9) Make Firefox Open on Startup 44
10) Changing On-Screen Keyboard Settings 44
11) Installing Custom On-Screen Keyboard 44
12) Installing Add-Ons for Firefox Interface 45
13) Removing Desktop Items 45
14) Locking & Removing All Settings 45
15) Revoking VHASDCESCREEN Administrator's rights 46
16) Test Locked Down Tablet 46

STEP-BY-STEP WITH SCREENSHOTS 48

1) Change the View for the Assessment 48
2) Download Keycall off of R Drive 48
3) Add Printer to the Tablet 50
4) Authorizing VHASDCESCREEN to Have Administrator's Rights 51
5) Prevent Microsoft Lync from Launching at Startup. 51
6) Install Mozilla Firefox 29.0 51
7) Disable Access to IE 53
8) Unpinning All Icons (Except Firefox) on the Task bar 54
9) Make Firefox Open on Startup 54
10) Changing On-Screen Keyboard Settings 57
11) Installing Custom On-Screen Keyboard 59
12) Installing Add-Ons for Firefox Interface 61
13) Removing Desktop Items 65
14) Locking & Removing All Settings 66
15) Revoking VHASDCESCREEN Administrator's rights 71
16) Perform the final lockdown step. 73
17) Test Locked Down Tablet 75

SAMSUNG TABLETS MAINTENANCE & TROUBLESHOOTING STEP-BY-STEP GUIDE 76

Reauthorize VHASDCESCREEN to Have Administrator's Rights 76
Backdoor to gpedit When Search Disabled 76
Startup folder not showing up in All Programs list 78
Cannot Add Shortcut in Startup Folder 79
Right-Clicking Does Not Do Anything (No Context Menus Available) 80
Keycall Error Message upon Installation 80

ATTACHMENT - APPROVAL SIGNATURES 81

1.0 Introduction

Mental Health eScreening (MHE) is a software application that automates the manual, paper-based, process used for screening Veterans in VA healthcare settings for mental health issues. MHE, a tablet-based screening tool, was created to accelerate and improve Veterans' access to VA mental health services. The tool accelerates the patient enrollment process by allowing clinicians to perform patient-directed screening with real-time scoring and chart note generation.

The application exchanges data directly with VistA, by pulling open clinical reminders, pulling Veteran identification and demographic data, inserting Veteran assessment data in the form of notes, and closing clinical reminders based on completion of assessments. Additionally, it creates new clinical reminders and inserts health factors based on the eScreening results.

After completing the screening, a Veteran receives an immediate summary report with individualized feedback and schedule reminders of upcoming appointments.

A data export feature allows the clinician to export selected assessments in either an Excel or CSV format to other applications. The data can be exported in identifiable or de-identified format.

1.1 Research Pilot Findings of MHE Benefits

Mental Health eScreening Research Pilot
For the last two years, members of the Center for Excellence in Stress and Mental Health (CESAMH) have been using eScreening for Operation Enduring Freedom/Operation Iraqi Freedom/Operation New Dawn (OEF/OIF/OND, also known as OOO) Veterans enrolling in VA Health Care in San Diego. CESAMH has also been tracking OEF/OIF/OND Veterans for depression, suicide risk, PTSD, and more.

Findings from the Research Pilot
CESAMH found that about half of the newly enrolled had risk factors for suicide, indicating the need for immediate clinical follow-up. Additionally, many Veterans had symptoms of depression or anxiety, and the majority were in physical pain.

Screening times were compared between Veterans using paper packet forms versus Veterans using CESAMH tablets to self-assess during enrollment. Almost all of the tablet-using Veterans had their screenings documented an average of 19 days sooner than the Veterans who used paper packet forms. Additionally, almost all of the tablet-using Vets who wanted help were able to speak with a clinician within 3 days, versus 2-3 months with the old paper packet forms. This is a fantastic leap forward in patient care.

eScreening:

- was preferred by both Clinicians and Veterans.
- increased access to mental and physical health screening.
- created significant improvement in many areas of clinical care, such as:
    - timely triage to appropriate services (approximately 40% of Veterans need immediate follow-up with the Suicide Risk Assessment).
    - the ability to monitor treatment outcomes over time.

- increased encouragement of Veterans with immediate personalized feedback.
- greater overall Veterans' satisfaction due to an increase in trust regarding their needs.

The administrative benefits of eScreening are:

- increased screening capacity for the VA (and improved rates of VA-mandated screening),
- the ability to monitor treatment outcomes over time (greater efficiency),
- a reduction in time for clinical care and documentation (cost savings), and
- increased quality of care without increasing staff (cost savings).

1.2 Purpose

This document serves to plan the implementation of MHE within the OEF/OIF/OND Care Management Programs in the VA's San Diego location, including Enrollment, Mental Health Access Clinic, and Primary Care.

1.3 Project Oversight

CESAMH reports directly to the Acting Chief Consultant for Mental Health Services. It receives oversight by the VISN Mental Health Lead, and ultimately, Mental Health Operations.
MHE's executive sponsor:

- Niloo Afari, PhD, Division Director,
  Mental Health Integrative and Consultative Care Services,
  VA San Diego Healthcare System;

  Director of Clinical Affairs,
  VA Center of Excellence for Stress and Mental Health,
  Associate Professor of Psychiatry,
  UCSD Health System.

Coordinating officials:

- Clint Latimer (FAC-P/PM, COR, VHA Innovations)
- James Pittman (Social Worker, Department of Social Work)
- Elizabeth Floto (Project Manager, CESAMH)

The implementation work is performed by Information Innovators Inc. (Triple-i), a contractor team of engineers and developers under VACI project 20388, contract VA118-11-D1002.

1.4 System Overview

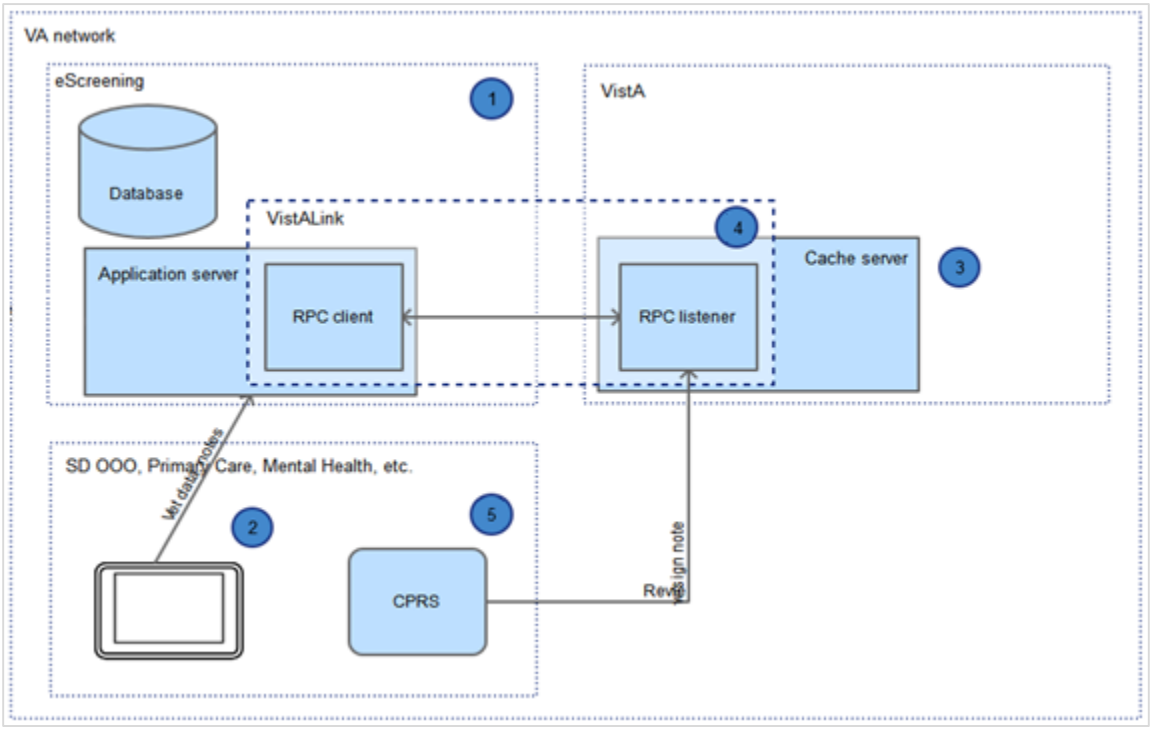
MHE consists of three principal components, all based on open-source web technology:

- a forms editor for designing assessments and note templates,
- a Veteran assessment portal that works for Firefox on Samsung and iPad tablets, and
- a web-based administrative dashboard (staff portal) that allows clinicians to monitor assessment progress, view assessment alerts, review completed assessments, and publish generated reports to VistA/CPRS. The dashboard also handles exporting of assessment data for data analysis purposes.

Both the dashboard and the forms editor are under the same staff portal, but technical administrators are the only ones that have access to the forms editor. The staff portal runs inside of the VA on a tablet or laptop computer web browser.

The Veteran assessment portal is web-based and requires wireless access for tablets. All communications between the Veteran assessment portal and the eScreening server are securely encrypted, and no patient data is stored on the tablet running the assessment.

The eScreening server will run from the San Diego VA Medical Center and will be protected by VA security and firewalls. All listed components are behind the VA firewall. Outreach could only take place through a secure VA VPN connection.



Mental Health eScreening Architecture

Legend:

❶ The eScreening system resides in the San Diego VA Medical Center and consists of a web application, web services, and a database.

❷ Clinicians and Veterans access authorized portions of the web application from San Diego VA Medical Center facilities such as the Primary Care program location.

❸ eScreening reads limited patient identification and demographics data from VistA, and writes assessment results to VistA.

❹ eScreening integrates with VistA via VistALink entirely on the VA network.

❺ Staff use CPRS to view and sign assessment notes, and maintain patient records.

1.5 Scope

This document covers the planning, deployment, and activation of system implementation, and implementation metrics for the San Diego location. It does not include planning for the optional VISN 22 deployments.

1.6 Stakeholder Approach

Engagement of Stakeholders:

1. Identify and engage leadership in order to appropriately obtain support. Be sure to include, among others:
    - Facility Chief Information Officer
    - Chief Health Information Officer
    - Information Security Officer
    - Privacy Officer
2. Identify main points of contact (POCs) and other stakeholders who would like to be and need to be kept informed.
3. Collaboratively develop a process based on current model.
4. Collaboratively identify individual screens to be utilized in care settings.
5. Identify primary users of eScreening and engage them as needed to gain support.
6. Develop a program specific strategy based on feedback from primary users and leadership.
7. Demonstrate the eScreening application on a regular basis to build familiarity and make changes as necessary for customer satisfaction.
8. Provide user and administrator training.
9. Implement the application via pilot testing and make necessary corrections via defect/bug fixes.
10. Iteratively collect feedback and make modifications as required.

2.0 Assumptions

2.1 Technical

Type	Description
Security	VA will secure the tablets via an operating-system level password, MDM, and either a native (supervised) or a third party application-based kiosk mode. Staff can unlock the tablets during operation or for maintenance, however, Veterans can only access the application via unique credentials.
WIFI access	The tablet will access the web application via WIFI.
Network access	The tablet will access the web application over port 443. The application will access VistA.
VistA access	The application server on the VA network will access the SD VistA system, including reading/writing data for a specified Veteran.

Administrative access	VA will provide RDP administrative access to the individuals responsible for maintaining the application server components (web server, etc.)
Tablet maintenance	VA will provide a means to update and charge the tablets when they are not in use.

2.2 Organizational

Type	Description
Physical security	VA will provide physical security for the server and tablets.
Administrative staff	VA will provide staff to operate the program, including helping the Veterans to use the tablets, and operating the administrative dashboard.
Support staff	VA will provide IT staff to support the program at the hardware and network level.

3.0 Roles and Responsibilities

3.1 Implementation Team Information

Group	Role
CESAMH	Lead all coordination activities with support from Triple-i.
VACI	Oversee contractual compliance.
Region 1 OIT	Oversee regional IT compliance.
VISN 22 OIT	Oversee VISN IT compliance.
SD OIT	Manage hardware deployment and security, and network engineering.
ISO and Privacy Office	Information security compliance and monitoring.
Information Innovators Inc. (Triple-i)	Development and administration of the application.

3.2 Points of Contact

Name	Location	Department	Role	Contact
Niloo Afari	San Diego, CA	Mental Health	Executive sponsor	858-249-9806
James Pittman	San Diego, CA	CESAMH/ Social Work	SME/Co-Sponsor	858-518-6982
Elizabeth Floto	San Diego, CA	VHA	Project Manager	858-552-8585 x2950
Clint Latimer	Santa Rosa, CA	VHA Innovation Program	VA Project Coordinator/ COR	650-814-3660
Darryel Simmons	San Diego, CA	OIT	Facility CIO	858-523-8104
Randy Quinton	Long Beach, CA	VA VISN 22	Deputy Network Director VISN 22	818-535-3754
Emanuel Carter	San Diego, CA	VA OIT	IT Supervisor	858-353-3689
Daniel Tang	San Diego, CA	VA OIT	Lead Tech	858-642-1104
Jesse Christmas	San Diego, CA	VA ISO	Information Security Officer	858-642-6200
Steven Colbird	San Diego, CA	Inventory Control	Supervisor, General Supply	858-249-9093
Melinda Lee	San Diego, CA	VHASDC	VistA CAC	858-642-1073
Kevin DeZorzi	Phoenix, AZ	Region 1 OIT	Division Chief R1 Field Development	602-290-8015
Radhika Kumar	Washington DC	Contractor	Project Manager	703-579-7150
Robin Carnow	Washington DC	Contractor	Technical Lead	301-244-8892

3.3 San Diego Key Positions

Social Work	
OOO Program Manager	858-642-3593
Transition Patient Advocate	858-642-3782
Case Managers	
Case Manager	858-642-3615
Case Manager	858-552-8585 x2913
Case Manager	858-642-6467
Mental Health	
ACOS Mental Health	858-642-1206
Impact Unit Leaders	858-642-3678
Impact Unit Leaders Psychologist	858-552-8585 x2976
Mental Health Access Clinic Staff	858-552-3723
Aspire Center	
Chief of Aspire Center	619-497-8454
Medical Director of Aspire Center	619-497-8454
Clinical Team	
Social Worker	619-497-8456
Clinical Psychologist	619-497-8455
Clinical Psychologist	619-497-8488
Clinical Psychologist	619-497-8488
Primary Care	

Chief of Primary Care	858-552-7475
Lead Clerk	858-642-3291
Lead LVN	858-623-1865
Nurse Lead	858-642-3643
Physician	858-552-7475

3.4 Coordination

The CESAMH team will lead all coordination activities with support from Triple-i.

3.5 Site Notification of Product Release

Site notification of product release	
Group	**Task**
VA Office of Information Technology (OIT) or CESAMH	During pilot testing of MHE, VA Office of Information Technology (OIT) or CESAMH will send an email to all pilot testers informing them of any upgrades or patches to the system.
CESAMH team	After eScreening has successfully completed pilot testing and has been approved for implementation by VA OIT and Privacy, the CESAMH team will email the users of eScreening at OOO facilities (such as Clinical Application Coordinators), and copy VA OIT and Privacy, of the use of MHE.
VA OIT	Any subsequent updates, upgrades, patches, or other changes to the system will be the responsibility of VA OIT to inform the users of the system via email.

4.0 Overall Specifications

4.1 Rollout

The San Diego pilot will run six months after delivery of the full prototype.

4.2 Defect and Bug Support

Defect and bug fix support began on June 15, 2015 and will continue for the duration of the pilot. Triple-i will provide defect and bug fix support to the VA as the eScreening capabilities are implemented. At the completion of each defect correction, Triple-i will apply any corrective updates to the code and if needed, make corresponding updates to documentation such as user and training guides. Any defect correction will be implemented for the affected code at all previous implementation sites.

Defects may be identified by the Government Project Manager, users, business owners, Software Quality Assurance evaluation, or through the existing defect reporting chain.

After the eScreening pilot testing has been completed and fully integrated, the SD IT will provide support to the hardware.

4.3 Training

Triple-i will perform user level and administrator level training to address the use, management, and administration of the eScreening capability. Triple-i will provide training materials that outline the purpose and utility of the eScreening application and provide the knowledge and skills necessary to utilize the full functionality of the application, and to manage and administer it.

Training materials will be provided for each user trained and will include:

- Lesson Plans.
- Presentation slides.
- User training manuals that describe the eScreening application, its use and all of its functionality.
- Graphic images, as appropriate.
- Questions and answers that will effectively evaluate trainee understanding and the comprehension of training materials and concepts.

Following COR approval of the training materials and as part of the pilot installation, Triple-i will provide remote training for up to one-hundred (100) users. The training will be spread across multiple sessions during multiple days and shifts.

Additionally, Triple-i will provide training and education for up to ten (10) clinical program technical administrators. Training shall address the use, management, and administration of the Program level dashboard.

4.4 508 Compliance

The Triple-i test team will test 508 usability and resolve any issues. Any unresolved issues will be categorized and escalated to the eScreening PM. The Triple-i QA team will work with the eScreening PM and the development team to resolve open issues and make sure that the system meets all the requirements specified in the Contract and the Performance Work Statement.

4.5 User Acceptance Testing

4.5.1 Preparation

Team Triple-i will create a User Acceptance Testing (UAT) Plan which details the steps required to validate the developed eScreening system. The Triple-i QA team will develop and document UAT cases and procedures, and will submit drafts for review by the COR and VA program management. When due, the final versions of the UAT Plan and Procedures documents will be submitted to the COR and VA program management. The scope will be limited to the three San Diego pilot facilities.

4.5.2 Deployment

The application is built incrementally and tested at the end of every sprint. After closing a sprint, that functionality is released in a UAT environment for the Product Owner to test. If defects are

discovered, Triple-i developers will correct them, release the update, and the UAT can be repeated. After the Product Owner's approval, the application can be released into the Production environment of the respective pilot facility.

4.5.3 VA UAT

The VA UAT staff will track defects and report them to the Triple-i Development Team. Triple-i will confirm the defects and either party may create a ticket. Test cases will be added if needed. Triple-i developers will be assigned to correct defects reported in the tickets. If a defect is severe enough to halt testing, an immediate priority will be raised and the Triple-i Team will begin repair immediately.

4.5.4 Post-UAT Issue Resolution

Triple-i developers will use defect logs to address any eScreening system defects discovered by the VA testing staff. After the removal of system defects, the Triple-i Team will deploy the update to the San Diego VA Medical Center facilities.

5.0 Transitioning Pilot to be run 100% by VA IT and Clinical Staff

5.1 Transition Overview

Upon conclusion, the pilot program will transition directly to VA OI&T. Triple-i will provide training and education for up to ten clinical program technical administrators (Healthcare System Technical Administrators). Training shall address the use, management, and administration of the Program level dashboard. See section 4.3 in this document for more information on training.

VA OI&T will begin maintaining the application and server. Application maintenance for MHE consists of routine maintenance for the application and operating system, and bug fixes for the application.

- For complete information on how to manage, operate, and configure the system to interoperate with the existing IT infrastructure at the pilot sites, consult the project's *System Administration Manual.*
- For complete technical information, server requirements, installation and administration to support the installed eScreening system, consult the project's *Server Manual*.

Both of the above documents are located in the MHE SharePoint and on the vacloud. An overview to these operations is provided below for convenience.

5.2 Maintenance

5.2.1 Routine Maintenance

In order to keep the application running correctly and comply with all VA security and stability guidelines, SD IT should perform database backups and operating systems updates regularly. For full details regarding routine maintenance, see the project *System Administration Manual*.

5.2.2 Database backups

The MySQL database should be backed up nightly, or on a schedule negotiated by program management and IT. The database backup should be scripted to perform a full or incremental backup to network storage external to the application server itself. For full details regarding database backups, see the project *System Administration Manual*.

5.2.3 Operating system updates

The Windows operating system should have Windows updates applied on the IT regular Windows maintenance schedule. For full details regarding operating system updates, see the project *System Administration Manual*.

5.2.4 System recovery procedures

For full details regarding crash recovery procedures and troubleshooting, see the project *System Administration Manual*.

5.2.5 Application configuration

Application settings are stored in configuration files on the server. These files contain values for things that need to be changed without redeploying the application, such as database or VistA addresses, or settings that can change the way the application operations. For full details regarding application configuration, see the project *System Administration Manual*.

5.2.6 Application or database code changes

In the event that a problem is reported that cannot be resolved through changing configuration, the application code will need to be changed. Application code consists of HTML5, JavaScript, and Java code for the web application component and SQL for the database component. For full details regarding application source code files and development tools, see the *project System Administration Manual*.

5.3 Software

The MHE system is composed of a web application and a database on the server, and web browsers on the client. Internet Explorer 11 is the only browser approved by OI&T, so all desktops in a clinic needs to be IE 11.

The web application is accessed via a browser and consists of user-visible screens, and background web services that are used by the browser to send and receive data transparently. The web application inputs assessment data from users and stores it in the database, making it available to clinicians for reporting and monitoring.

5.3.1 Server Software

The MHE web application is written in HTML5, JavaScript, and Java 7 (64b Oracle version). It is hosted on a web application server and is accessed by web browsers on computers and tablets. The application is based on the Java servlet API and must be run inside of a Java container server.

The application is configured by adding keys and values to properties and configuration files. Typical configuration entries include URLs and IP addresses that vary by installation, as well as options for how the system will run. For more information, consult the project *Server Manual* and the *Developer Environment Setup Guide*.

5.4 eScreening production deployment information

- Tomcat location:
  D:\apps\apache-tomcat
- Tomat Service Names:
  - tomcat-sdc-prod
  - tomcat-lon-prod
- Production Database Names:
  - sdc-prod
  - lon-prod
- The eScreening deployment directories are located at:
  D:\escreening
- Configurations for each of the Tomcat instances are located under:
  D:\apps\tomcatInstances

5.5 Creating a new eScreening instance

Each of the production instances of Tomcat are run individually. Follow the steps below to create a new instance (for example, tomcat-lon-prod).

5.5.1 Creating the Instance Tomcat Base Directory

The new base directory will contain all Tomcat work folders for the new Tomcat instance.

1. Using Windows explorer, navigate to:
   D:\apps\tomcatInstances
2. Copy and paste instance-template directory to this same directory
3. Rename the new directory using the convention:
   <3_letter_abbreviation>-prod
4. Update the instanceIDs.txt document with a new entry for this new instance with a new unique ID.
5. Edit the file in:
   <new instance directory>\conf\server.xml
   1. Update the following using Notepad:
      1. Server port to 81** where ** is the ID of this server.
      2. Http Connector port to 82** where ** is the ID of this server.
      3. AJP Connector port to 83** where ** is the ID of this server.
   2. Save and close the editor.

5.5.2 Installing Instance IIS Service

The following steps cover how to add a new service responsible for starting and stopping the new Tomcat instance.

1. Open up a terminal/shell with admin privileges (for example, right-click cmd.exe and select "Run as administrator")

2. If using power shell execute: cmd

3. Run: cd D:\apps\apache-tomcat\bin

4. Run: set CATALINA_HOME=D:\apps\apache-tomcat

5. Run: set CATALINA_BASE=D:\apps\tomcatInstances\<new instance directory>
   Here <new instance directory> is the name of the new base directory created in the previous section. Below "<new_instance_name>" is "tomcat-<new_instance_directory_name>"

6. Run: .\service install <new_instance_name>

7. Run: .\tomcat7 //US//<new_instance_name> --Startup=auto --JvmMx=2048
   The JvmMx=2048 sets the maximum memory to 2 GB. This setting should be calculated carefully so that the total amount of memory used by the system is not greater than the total physical memory. Also, the value should be large enough to adequately handle the expected load of the server.

8. To have the new service show up, open the Server Manager and press the F5 key.

5.5.2.1 Setting Tomcat Parameters

To edit the Tomcat parameters (e.g. JVM options) for the new instance:

1. Run: cd D:\apps\apache-tomcat\bin

2. Run: set CATALINA_HOME=D:\apps\apache-tomcat

3. Run: set CATALINA_BASE=D:\apps\tomcatInstances\<new instance directory>

4. Run: .\tomcat7w //ES//<new_instance_name>

5. Set the required JVM settings:
   1. Click the **Java** tab.
   2. Add these settings in the Java Options text box:
      Dfile.encoding=UTF-8
      Dserver
      XX:MaxPermSize=512m
   3. If this is a production instance, add:
      Dgov.va.med.environment.production=true

5.5.3 Adding Instance IIS Proxy Rule

To add a proxy rule which uses the URL of incoming client requests and routes the request to the correct Tomcat instance:

1. Start the new Tomcat service.

2. Open the IIS Manager.

3. Unfold: VHASDCAPP22 > Sites > 'Default Web Site'

4. Click **Default Web Site**.

5. Open URL Rewrite.

6. Click **Add Rules**.

7. Select **reverse proxy**.
   The port to use below is the 82** where ** is the server ID (for example, 8203 for the lon instance).

8. Set the following:
   1. Inbound field: localhost:82<server ID>
   2. Check off: Rewrite the domain names of the links in HTTP responses
   3. From field: localhost:82<server ID>
   4. To field: vawww.escreening.va.gov
9. Click **OK** in the Add Reverse Proxy Rules dialog.

10. Double-Click the new rule from the inbound requests.

11. In the Pattern field, enter: ^<instance_3_letter_code>$|<instance_3_letter_code>\/.*
    For example: ^sdc$|sdc\/.*

12. In the Rewrite URL field, enter:
    http://localhost:82<server ID>/{R:0}

13. Click **Apply** and go back to rules.

14. Close the IIS manager.

5.5.4 Creating an Instance Database

Each Tomcat site will have its own eScreening database schema. There are two MySQL instances running which manage various schemes:

- Test on port 3307
- Production on port 3306

These steps show how to initialize a new database schema:

1. Open the MySQL workbench.
2. Log into the instance, depending on the type of Tomcat instance being deployed (in other words, test or production).
3. Run the following to create the new database (replace *database_name* with the name of each database):
   CREATE DATABASE IF NOT EXISTS *database_name*;

4. Give the escrapp user permissions to build the new database by (replace *database_name* with the name of each database):
   GRANT ALL ON *database_name*.* TO 'escrapp'@'localhost';

5.5.5 Creating an Instance Deployment Staging Area

To facilitate simple, error-free eScreeing maintenance, each instance has a separate staging area where an instance manages version and database updates.

In the following steps, when <profile_name> is shown, replace this with the name of the Maven profile which has been created for this instance (for example, sdc-prod).

1. Start the **GIT** Bash program.

2. Run:
   cd d:/escreening
3. Review the code by running:
   git clone https://github.com/VHAINNOVATIONS/Mental-Health-eScreening.git <profile_name>-release

This operation will create a new directory with eScreening code. For example, the new directory might be called "sdc-prod-release".

1. Copy and paste the file deploy-template.sh
2. Rename the copy to:
   deploy-<profile_name>.sh
   For example: deploy-sdc-prod.sh

3. Edit the new file.

4. Set all of the instance-specific parameters.

5. Save the file.

5.5.6 Restarting Tomcat

If Tomcat is down, it can be restarted from the services menu. The service name is: tomcat_prod

5.5.7 Supporting Software

The application uses a number of common free/open source supporting software products. It runs on any modern 64 bit operating system, and will be delivered on Windows Server 2012.

Component	Product
Framework	Java 7 64 bit Oracle VM[1]
Web server	Apache Tomcat 7 servlet container
Database	MySQL 6.5 Community Edition
Operating system	Windows Server 2012 or 64 bit Linux[2] with at least 16 GB of RAM and 750 GB of disk space.[3]

5.5.8 Firewall

On the server, port 443 must be open in order for web browsers to communicate with the application.

Between the application server and VistA, the required ports must be open in order for the application server to perform relevant operations, including reading veteran identity and demographic information, reading and closing open clinical reminders for a veteran, and inserting assessment results and notes into the veteran's VistA record.

5.5.9 Client Software

The application is served from a web server (see server software section above), but runs in part within a web browser on the client computer or mobile device.
The client portion of the application is composed of HTML5 and JavaScript, and will execute in any browser that supports HTML5 and JavaScript. The PWS requires that we deliver an HTML5-based solution:
The eScreening application developed shall be designed to operate on the latest mobile iOS or equivalent operating system (OS) and be available in Hypertext Markup Language-5 (HTML-5) at the time of delivery, to ensure this application is OS agnostic.

IMPORTANT! The only browser versions that currently meaningfully support HTML5 well are IE10+, Safari 6+, Chrome 8+, FF 4+, and Opera 11+. Therefore: *One of these modern browser versions must be installed on the client machine/device. The browser's JavaScript feature must be enabled.*

5.5.10 VPN Software

The client device must have VPN software installed that works with VA's VPN capabilities, such as the latest Cisco VPN client. The VA installs and configures this software.

[1] Not tested on other Java VM.

[2] The pilot server will use SD IT's preferred operating system, Windows Server 2012.
[3] 1.2 TB of disk space and 16 GB of RAM will be provided on the pilot server.

5.5.11 Operating System

The application will run in any operating system on any computer or mobile device that can run one of the supported web browsers (see above). This includes Windows, MacOS, and mobile-based operating systems like iOS (iPad) and Android.

5.5 Hardware Physical Description

The physical eScreening hardware consists of one physical server and approximately 600 tablets. The eScreening application runs on the physical server in the San Diego VA Medical Center. Staff access the dashboard and designer components from VA workstations. Staff and Veterans access the runtime component from HTML5-capable browsers on tablet devices.

Specifications for the eScreening hardware

Item	Make	Model	OS	Memory	Storage	Location
Server	Dell	R420	Windows Server 2012	64 GB	1.2 TB (after RAID 10)	VASD data center
Tablet	Samsung	Slate	Windows 7 Enterprise	4 GB	118 GB	San Diego VAMC
Tablet	Apple	iPad2	iOS 7.1	512 MB	16 GB	Each program location

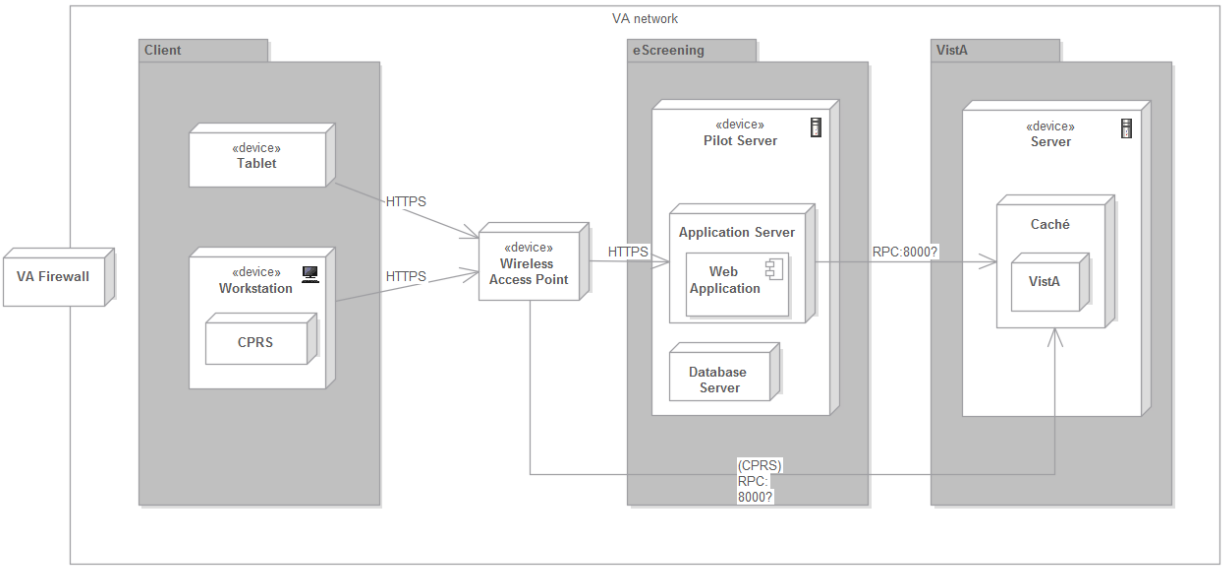
The application server hardware is a rack-mount server. It has the following rack and electrical footprint:

Element	Attribute
Form factor	2U
Power	Dual hot plug 550W power supplies, 2 x 15 amp 10 ft. wall plug

The server additionally contains 12 CPU cores (6 physical, 6 virtual), and can be upgraded to include another CPU for a total of 24 cores. The memory can be upgrade to a total of 384 GB 1600 MT/S over 12 DIMM slots. The internal storage can be upgraded to a maximum of 16 TB (8 TB usable via RAID 10).

The tablets connect to the server and the server connects to VistA. The tablets talk HTTP over TLS to the server via a SD VAMC 11g wireless network. The eScreening server communicates with Cache via RPC over port 8000. The diagram below shows all device communications, including type and bandwidth.

eScreening Hardware Connections



In OEF/OIF/OOO outreach scenarios, tablets connect to the VA network over VPN and MIFI. All communication between eScreening and VistA takes place behind the VA firewall.

See the Deployment Roles and Responsibilities table in Section 3.4 for details about who is responsible for preparing the site to meet these hardware specifications.

This system is not considered critical.

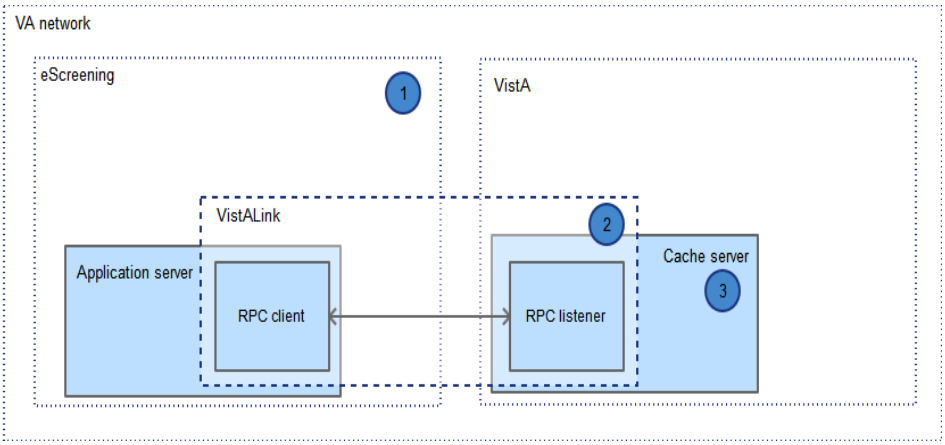
5.6 VistA Resources

The application integrates with VistA in order to exchange data with the veteran record, including the following operations on behalf of a veteran:

- Reading identification information
- Reading demographics information
- Reading and writing (e.g., closing or updating) active clinical reminders, health factors, and consults

Inserting assessment results as clinical progress notes (to be reviewed within CPRS) in a manner that will trigger VistA to generate consults and clinical reminders

The application runs on the VA network. Veterans and VA staff access the application via web pages over VPN or VA networks. The application allows the staff to pull some limited data (e.g., ID an demographics, open clinical reminders), and update the veteran's record with the results of his/her eScreening session. The application reuses existing RPCs rather than provide new ones that must be deployed via KIDS builds.



Legend:

❶ The eScreening application uses the VistALink Java client library

❷ VistALink provides bi-directional communication between the client and the server

❸ The Cache (M) server runs the VistALink listener

All communication between eScreening and VistA takes place behind VA firewalls via VA VistALink, an RPC framework that is part of the OneVA architecture. The VistA RPC that eScreening makes are not new; rather, we have identified the RPC that CPRS makes and are simply reusing them as fits eScreening.

5.6.1 VistA Proxy Account

The Proxy Account is the VistA service account with which the MHE application connects with VistA. The Proxy account is provided by R01 OIT. The Verify Code for the Proxy account cannot be set to never expire. The current way the Proxy Account is configured is by a server administrator who does the following:

1. Remote into VHASDCAPPS22 (or app server).
2. Stop the Tomcat server (go to Services, right-click the Tomcat entry, then select **stop service**).
3. Go to the deploy directory:
   a. $tomcat_dir/webapps/${escreening_package_name}/WEB-INF/classes.
   b. Open the gov.va.med.vistalink.connectorConfig.xml , then edit the second connector entry.
   c. Save.
4. Restart the server.

If you are configuring a new adapter, contact the VistA/M system's Information Security Officer and/or the VistA/M system manager to obtain the connector proxy user's credentials for the VistA/M system to which you want to connect. This information includes:

- Access/verify codes and the DUZ for connector proxy user
- VistALink listener port
- IP address of the VistA/M system

The sysadmin user must be configured with the correct station ID and DUZ in the eScreening database. Use mysql workbench and log in to the database, then run this sql command:

update user set vista_duz='…', vista_division='…' where user_id=1

5.6.2 SSL Certificate

The eScreening domain must be joined to the VA domain and an SSL certificate issued. For information on how to install the SSL certificate, click:

https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

The instructions are under the "Installing a Certificate from a Certificate Authority" section.

5.7 Network Resources

The client component of the application requires access to the server component over HTTPS (encrypted web protocol). Additionally, VA security requirements dictate that the client component must be able to make this connection from within a VPN session, using VA-installed VPN software, when operating outside of VA facilities.

5.7.1 Firewall

Port 443 to the server must be opened so that OOO clinicians and veterans can access the site internally from inside SD VA facilities, and externally from outreach events.
Internally, VA clinicians and OOO veterans will access the application from within the VA OOO facility via VA wireless networks. Externally, VA clinicians and OOO veterans will access the application at outreach events via WIFI or VA-controlled mobile WIFI networks only.

5.7.2 DNS

Internal and external DNS entries (e.g., escreening.va.gov) must be registered for the application based on the VA project manager's choice of domain names.

5.7.3 VPN

The client component must have VA VPN access in order to access the VA-based application server component from outside of the VA. The VA must provide the VA staff using the VPN software outside of the VA facilities with a VPN account. The VPN account has nothing to do with the application itself; rather, the encrypted VPN session simply provides connectivity between the client and server.

5.8 Facilities

The application server needs to be run within a data center environment that can support it, including providing power, cooling, and physical security. See section 5.5 for hardware specifications regarding rack and electrical footprint.

5.9 Tablet Management

5.9.1 Sanitation

Per reference SDVAMC MCM 118-33:

The tablets are considered non-critical items (devices that come in contact with intact skin but not mucous membranes). As such, they require low-level disinfection between each patient use. All eScreening staff are responsible for cleaning between each patient use with one of the following hospital disinfectants with tuberculocidal activity:

- EVS supplied spray cleaner (for example, Precise QTB or Clorox cleaner disinfectant)
- Dispatch with bleach
- CaviWipes
- Sani-Cloth Bleach
- Super Sani Wipes

5.9.2 Inventory

Per reference SDVAMC MCM 90-02:

When	By whom	Tracking method	Details
Nightly	Clinic's lead supervisor	Checklist	Kept by the lead supervisor.
Monthly	Clinic or service manager	Checklist	Kept by the clinic or service manager
Yearly	Dr. Afari, initially. Eventually to be transferred to IT or other personnel TBD.	Bar code scanner	a) The Chief, Logistics Officer will notify the responsible official, via electronic mail notification, at least 15 days in advance of their scheduled inventory that an inventory is due. A copy of the applicable EIL along with a bar code scanner will be furnished by Materiel Management (90M) for use in taking the inventory. b) Responsible Officials will conduct a complete physical inventory of the property with which they are charged within 15 days (20 days for EILs with 100 or more line items). In order to conduct the inventory, the EIL official or designee will contact Materiel Management (90M) to schedule the use of a bar code scanner. When the employee arrives in Materiel Management, he/she will be given instruction in the use of the scanner. In the event that leave (annual, sick, sabbatical, etc.) is approved at the same time an inventory is due, attempts shall be made to complete the inventory prior to the beginning of leave. If this is not feasible, the Responsible Official should request an extension of up to 30 days from the Chief, Logistics Officer (90).

5.9.3 Missing tablets

Per reference SDVAMC MCM 90-03:

1 In the event a VA employee detects a missing or damaged piece of property, they will immediately report the situation to the responsible individual (supervisor or Equipment Inventory Listing Custodial Officer). Upon report of a missing item, the responsible individual will conduct an immediate search of the area in an attempt to locate the missing property and question individuals concerning their knowledge of the missing item or circumstances surrounding the damaged property. If the missing item contains sensitive information, the Information Security Officer must be notified within 59 minutes after realization of loss by the employee. Employees failing to report, and supervisors failing to initiate a ROS, may be subject to disciplinary action.

2 If unable to locate the missing property, the responsible individual is to immediately notify Logistics who will initiate VA Form 90-1217, Report of Survey. If suspicious evidence exists or the missing items total $5,000 or more, the responsible individual is to also contact the VA police and the VA police will complete VA Form 1393, Uniform Offense Report (UOR). The VA police investigating officer will review and incorporate into the UOR all related records in cases of reported loss to include outstanding repair service records, as well as the loans from the VA file and property pass file. The VA police will then forward the completed UOR to the Chief, Logistics Officer no later than three workdays from the discovery of the missing or damaged property. The completed UOR will then be incorporated into the ROS folder along with VA Form 90-1217.

3 The Chief, Logistics Officer will assign a ROS surveying official for all items below $5,000. If the Item/items are worth $5,000 or more or if the assignment of pecuniary liability is likely, the Chief, Logistics Officer will establish a board of survey. Both are required to be assigned within five workdays after notification by the responsible individual of the missing items. The ROS, along with accompanying information (e.g., a police report; or statement from an interested party; or a Security Operations Center report from the Information Security Officer on whether or not the item could or did contain sensitive data) will be forwarded to the Approving Official for review and approval of the personnel assigned to conduct the ROS investigation. The Approving Official may not be any grade lower than the Associate Director.

5.9.4 Disposal

Per reference SDVAMC MCM 118-22:

The tablets do not store sensitive data or any data from patient use. If the device becomes inoperable, follow hospital biomedical memorandum for disposal.

5.9.5 Samsung Tablet Security Steps

See Appendix B in this document.

5.10 Personnel

The personnel roles needed to operate the application are provided here along with basic tasks.

Tasks	Roles			
	Healthcare System Technical Admin.	**Clinician**	**Assistant**	**Veteran**
Log in	Y	Y	Y	Y
Create an assessment	Y	Y	Y	Y
Edit an assessment	Y	Y	Y	Y
Delete an assessment	Y	Y	Y	N
Save to VistA	Y	Y	Y	
Dynamic selection of clinician for individual assessments	Y	Y	Y	
Change an Assessment in an error state	Y	N	N	
Delete Error Assessment	Y	Y	Y	
Print/Email (to secure portal) Patient Summary	Y	Y	Y	
View Dashboard of active assessments with alerts	Y	Y	Y	
Edit User Forms	Y	N	N	
Manipulate and edit templates, and the system's interactions with VistA	Y	N	N	
Export data for Program Management	Y	Y	Y	
Edit Users who can access the system	Y	N	N	

6.0 Implementation Tasks and Activities

6.1 Operations and Support

OEF/OIF/OND Care Management Programs provide case management and care coordination for severely ill, injured, and impaired combat Veterans. The programs also assist in ensuring a smooth transition of health care services for returning service members and Veterans.

Although all of the San Diego programs fall under OEF/OIF/OND, the care scopes vary due to each location having a distinct administrative and clinical team configuration as well as physical layout. Given these differences, each program has unique considerations for the implementation of the eScreening application.

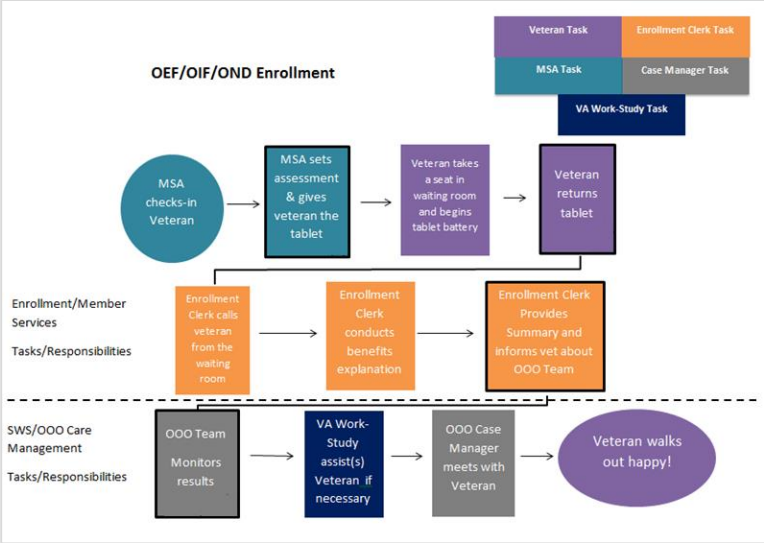
To analyze and optimize the workflows, Team Triple-i gathered requirements from targeted project stakeholders during interview-style meetings. Program stakeholders, CESAHM staff, and clinical champions in each care setting also contributed requirements, and feedback from staff.

Inevitably, there will be cases where a Veteran is unable to, or refuses to, take part in eScreening. These situations may include Veterans with impairments such as diminished vision, amputation, traumatic brain injury, drug or alcohol detoxification (delirium tremens), and other problems. Veterans whose CPRS record carries a SAIL flag should not be given a tablet; they present a danger due to aggressive behavior and could use the tablet as an instrument to harm others. If a Veteran refuses to accept an eScreening tablet or is otherwise unable to do so, nurses and healthcare providers should conduct clinical reminder collection by standard protocol.

6.1.1 OIF/OEF/OND Care Management

OIF/OEF/OND Enrollment/Member Services operates on a walk-in basis.

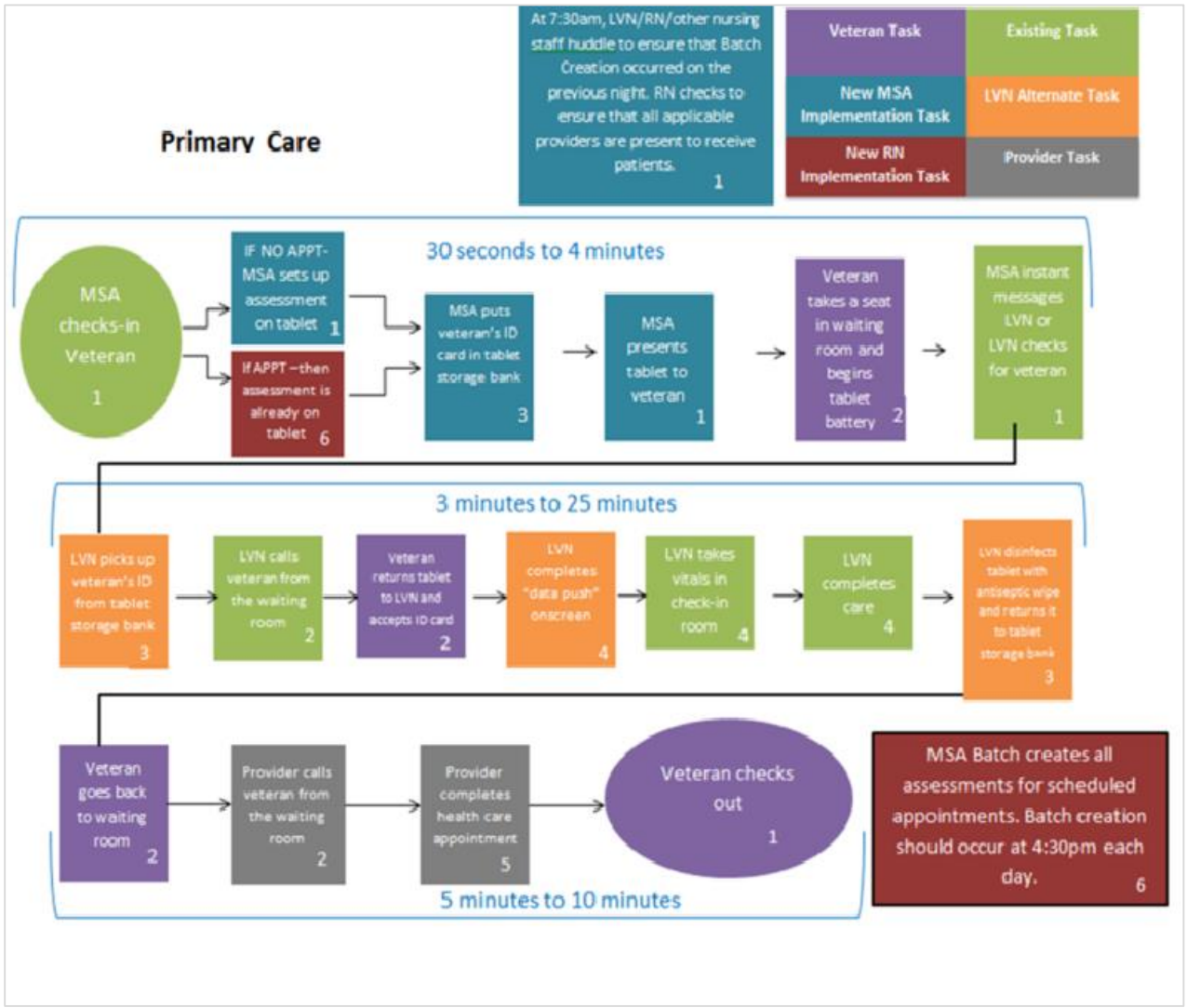
OIF/OEF/OND Enrollment Process Flow



6.1.2 Primary Care

- eScreening should precede all Primary Care appointments which fall on Tuesday through Friday, after 9am.
- An RN (or MSA) belonging to each pilot provider's Patient Aligned Care Team (PACT) should attempt to create assessments for all appointments scheduled on the following day. Creation should occur daily at 4:30PM or just before COB.
- Veterans must arrive at least 10 minutes prior to the scheduled appointment time in order to receive a tablet for eScreening.
- Veterans with CPRS records containing a SAIL flag must never be given an eScreening tablet.
- Some veterans may be physically unable to use the eScreening tablet. Use your best judgment.

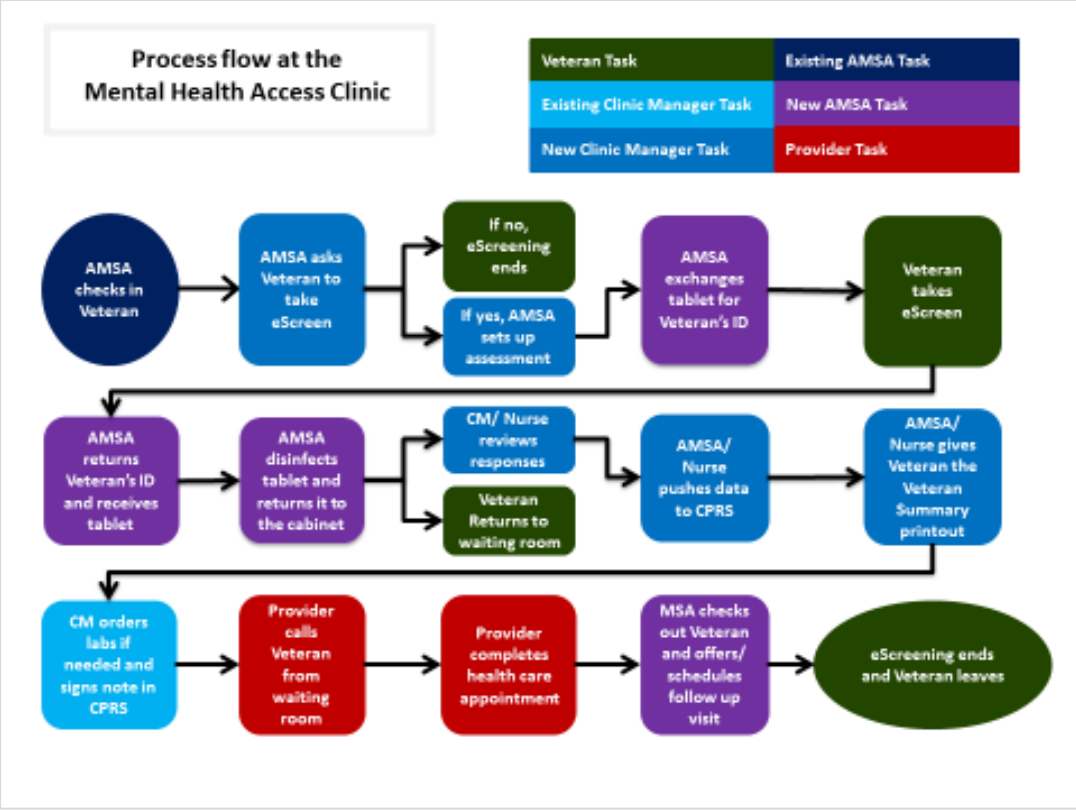
Primary Care Process Flow



6.1.3 Mental Health Access Clinic

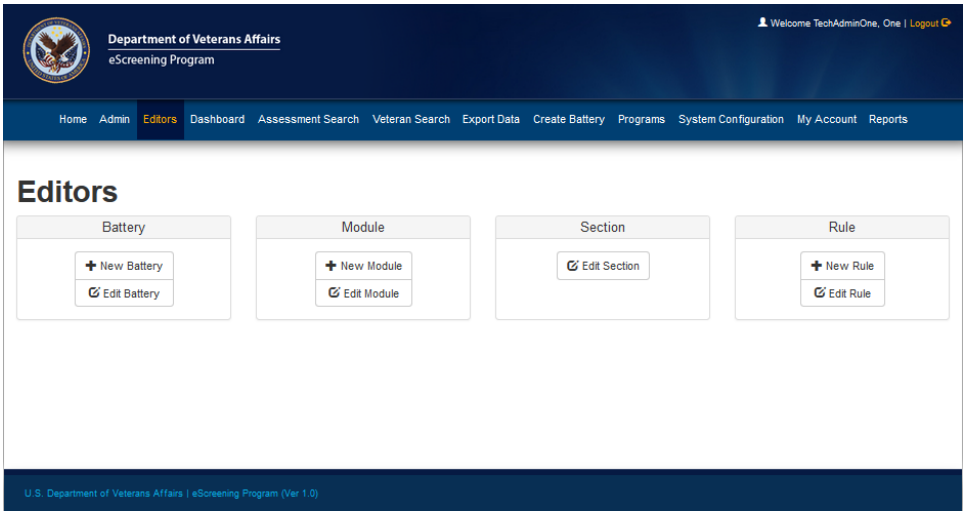
MHAC functions basically as an ER for psychiatric problems. Veterans presenting at the MHAC may be established patients at this clinic, or not, and may be undergoing an emotional crisis. The Clinic Manager or AMSA can suggest eScreening as warranted on a case-by-case basis.

MHAC Process Flow



6.2 Entering and Editing Assessments by VA professional staff (Customizing MHE for your clinic)

Mental Health eScreening takes the standardized paper forms packet that your clinic uses to screen and assess Veterans for services and support related to mental health issues, and translates it into an online system which partially automates the process. Because clinics vary in the paper packet forms that they use, MHE was designed in a way that lets you customize it for your clinic. The place to do this from is the Editors tab, which is available to the Healthcare System Technical Administrator (HSTA):



The HSTA can work with batteries, modules, sections, and rules. Batteries, also known as assessments, contain modules. Modules contain the questions the Veteran will answer to complete eScreening. The questions can be edited, created, and deleted. The HSTA can also manage the sections containing the modules, the modules, templates, formulas, and rules.

When your clinic converts to using MHE, you will be provided with the latest build of software. It will contain pre-grouped batteries, modules, and sections. It may not be necessary to make changes to these groups. In case that it is, full details for customization are provided in the *Technical Administrator Training Guide*. Below is an overview that allows you to understand the basic concepts for the purpose of planning with your staff and HSTA.

6.2.1 Batteries (Assessments)

A battery, also known as an assessment, is a customized collection of modules. The words "battery" and "assessment" are used somewhat interchangeably. Generally, a battery is called an "assessment" from the clinical side, and presented to the Veteran as a "battery". Therefore, a clinician may perform an "assessment search" in order to find and review any "batteries" a particular Veteran has taken. They are the same thing. Clinicians can also create batteries for walk-in Veterans, and create batteries by the batch for a day's appointments.

From the battery editor, the HSTA can:

- Create a battery (Click **+New Battery**, then populate the title and description, then click **+** and **>** to move modules into the **Assigned Modules by Section** area, then click **Save**.)
- Edit a battery (Click **Edit Battery**, then click **Edit**, then assign sections and modules to or from the battery.)
- Disable a battery (Click **Edit Battery**, then click **Edit**, then select the **Disabled** check box.)
- Manage templates (Click **Edit Battery**, then click **Edit**, then click **Manage Templates**, then click **Edit**, **Delete**, or **Create** for the template you want.)

6.2.2 Modules

A module is a customized container of questions. Modules correspond to groups of paper packet questions. Most modules are self-evident, such as the Presenting Problems Module and the Basic Demographics Module. Some modules are in the form of clinical reminders, such as the Homelessness Clinical Reminder Module.

From the module editor, the HSTA can:

- Create a module (Click **+New Module**, then populate the title and section, then add questions.)
- Deactivate a module from a battery
- Edit a module (Click **Edit Module**, then click **Edit**, then edit the title, selection, and description.)
    - Add, edit, or remove questions' and answers' properties in the module
    - receive validation messages to aid with correct formats
    - adjust page breaks and the questions' display order
- Create and edit formulas (Click **Edit Module**, then click **Edit**, then click **Manage Formulas**.)
- Create a template to be associated with the module (Click **Edit Module**, then click **Edit**, then click **Manage Templates**.) Some examples of templates are:
    - CPRS Note Entry template – generates the body elements for the CPRS Note
    - CPRS Note Headers and Footers – generates header and footer elements
    - VistA Questions and Answers template – generates the Q&A text for the CPRS Note
    - Veteran Summary Printout Entry template – generates the body elements for Printout
    - Assessment Welcome – generates the Veterans' welcome-to-the-system message

About Questions

Questions are edited in the module editor. For example, you may want to change a question in the Identification module. The HSTA can edit the question, and can also limit the answer. For example, if the question asks for a phone number, the answer can be structured to only accept numeric feedback. Questions can also be reordered in their presentation in the module by dragging and dropping.

There are six types of questions and an additional one in instruction format. The type of question being asked, and the number of possible answer choices available will help you and the HSTA select the proper format to use. For example, use a Free Text question for requesting information that is different for most Veterans, such as date of birth, or weight.

For guidance on choosing question types and detailed instructions for editing questions, see the project's *Technical Administrator Training Guide*.

About Formulas

The module editor provides the capability to use formulas to create complex relationships between multiple existing data elements in a module. Using the formula editor, the HSTA can take existing data from the answers that Veterans provide and build alternate elements based

upon these answers, applying a full range of mathematical operations. These new data elements are stored in variables which are available for use elsewhere in the templates--for display, creating alerts, measuring a Veteran's progress, or even for use in other formula creations. Formulas can be added or edited for a module, so that defined formulas can be used in templates and rules. The HSTA can create and edit formulas based on variables, operators, and parenthesis; edit a formula's name and description; and select variables from listings filtered by type. The list can include questions, answers, formulas, and custom variables.

About Templates

Templates can be managed from the module or the battery editors. Block types for If, Text, and Table are provided. Selecting a check box for Graphical Template provides the tools for adding intervals and extra axis value, graphing a maximum value, and including data from your choice of how many months. The HSTA must select a variable; there is a choice of question, custom, or formula.

6.2.3 Sections

Sections contain groups of similar modules. The purpose of a section is to make it easier to manipulate modules while constructing a battery.

The number of modules in a section vary. For example, the section called *Identification* contains only the Identification module. However, the *Demographics and Social Information* section contains nine modules:

- Presenting Problems
- Basic Demographics
- Education, Employment & Income
- Social Environment
- PROMIS Emotional Support
- Homelessness Clinical Reminder
- Pragmatic Concerns
- Advance Directive
- Spiritual Health

As you can see, all of the modules in the section contain questions which bear on demographics and social information.

6.2.4 Rules

Rules can be added to the system to trigger a given set of events, for example, so that Veteran responses can be monitored and events (such as a dashboard alert) can fire when triggered. Event types that can be added are consults, health factors, dashboard alerts, and the ability to show follow-up questions. The HSTA can:

- Add rules and delete them
- Edit the name of a rule
- Edit the rule's condition by selecting variables to use in the condition
- Add events to a rule or remove them

6.3 Outreach scenarios

The eScreening server runs from the San Diego VA Medical Center and is protected by VA security and firewalls. All listed components are behind the VA firewall. Currently, outreach can only take place through a secure VA VPN connection or VA authorized MIFI.

For roles and responsibilities, see section 3.4 in this document.

For purposes of planning, treat an outreach like you would a transition to another clinic. Engage site participants; create a workflow; ask questions; walk through steps of the event, and generally follow the section in this document on transitioning to remote assessments.

6.4 Transferring tablets to a different facility

San Diego Inventory Control (Steve Colbird) will complete VA 134 Form and VA 2237 and submit to the receiving facilities' Logistics Departments.

6.5 Training

CESAMH will perform user level and administrator level training to address the use, management, and administration of the eScreening capability. Triple-i will provide a training plan, technical administrator and general user training manuals, user guides, PowerPoints, and one-page guides.

Ongoing training support may include the following features:

- **Training material updates**: Updates to the functionality of the eScreening application resulting from enhancements, fixes, or requirement changes are anticipated. The Training Team will be responsible for updating training materials.
- **Onboarding**: Ideally, eScreening application training will be incorporated into onboarding training for new staff.

6.6 Activation

After all pilot testing has been completed to include all defect and bug fixes implemented, and the COR has accepted the application, eScreening will be made active for use.

6.7 Support

For general support, contact:

Liz Floto, 858-552-8585 Ext. 5550, Elizabeth.floto@va.gov

Matthew Morgan, 858-552-8585 ext.5557, Matthew.Morgan@va.gov

VA OI&T and the SD IT will provide support to the hardware after pilot testing has been completed and fully integrated.

7.0 Transitioning to remote assessments (from standard practice to using MHE)

7.1 Planning the Transition

Standard practice varies among VA clinics. These steps present a general outline for transitioning.

1. **Engage the clinic leadership.**
   The critical first task is getting their help to identify an employee in the hospital system who can serve as a superuser to train a technical administrator to take over support.
2. **Work with clinic staff to map the workflow.**
   Conduct a planning meeting with one staff person per role in the clinic. Having a staff member representing each role provides invaluable feedback regarding what steps may or may not work, and how the workflow may be amended for best results.
   This also promotes buy-in among the staff, and good public relations when the staff returns to their clinic and discusses the program with coworkers.
   In addition to mapping the workflow, collect the materials needed for the particular clinic. This will be the packets of module needs, questions, and clinical reminders that the technical administrator will use to customize the system.
3. **Create training materials and PowerPoints showing the new workflow.**
   Original materials can be retrofitted to serve.
4. **Prepare to train staff.**
   Create a checklist of staff needing training so that everyone is included. Track the training attendance and follow up later.
5. **Train staff.**
   Provide materials, conduct the training, and hold a Q&A session. Follow up on any questions you cannot answer.
6. **Transition – final checks**
   Personally check that the hardware is working. Have support for the hardware in place. Make sure that key personnel are trained and ready to go. Make sure that key personnel do not have remaining questions. Provide ongoing support and availability.
7. **Wellness check**
   Contact clinic leadership. Interview them for pros and cons of the procedure; identify sticking points that can be fixed.

7.2 Best Practices Suggestions

The Operation Enduring Freedom/Operation Iraqi Freedom/Operation New Dawn (OEF/OIF/OND, also called “OOO”) Care Management Programs provide case management for all severely ill, injured, and impaired combat Veterans. The programs also assist in ensuring a smooth transition of health care services for returning Veterans.

Although all of the San Diego deployments fall under OOO, each location has a distinct administrative and clinical team configuration as well as physical layout, and therefore, unique considerations.

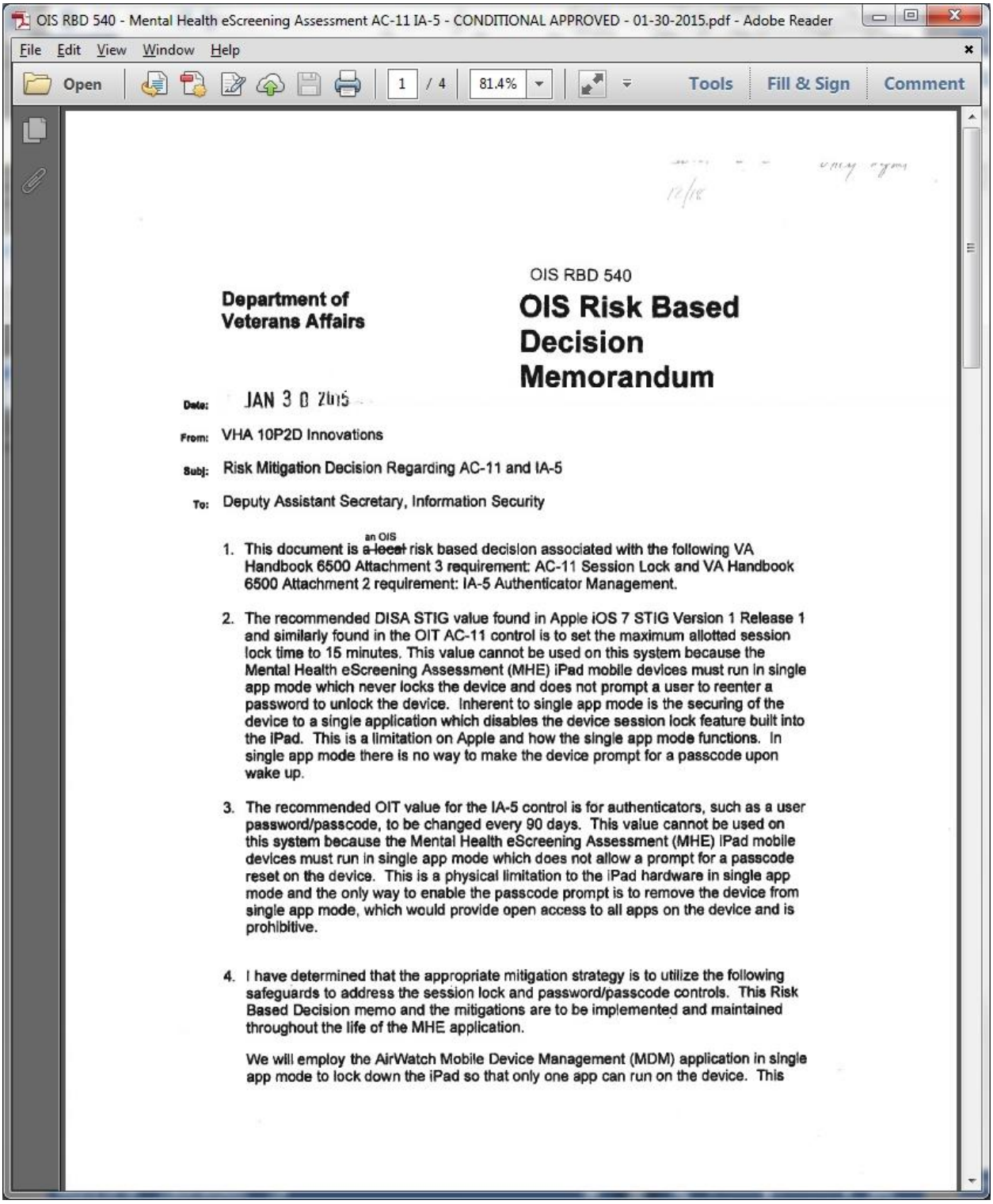
Overall program workflow considerations:

- We identified integration of eScreening into the enrollment process as a best practice. Greater integration helps to ensure that Veterans do not leave after enrollment or miss a step in the process. However, it's understood that not all locations will be able to incorporate eScreening into the enrollment process.
- The types of staff members vary at each location. Future best practices will need to be developed around who should conduct the screening, perform administrative functions and provide direct care to the Veteran.
- Inevitably, there will be cases where a Veteran is unable to, or refuses to, take part in eScreening. These situations may include Veterans with impairments such as diminished vision, amputation, traumatic brain injury, drug or alcohol detoxification (delirium tremens), and other problems. Additionally, Veterans whose CPRS record carries a SAIL flag should not be given a tablet; they present a danger due to aggressive behavior and could use the tablet as an instrument to harm others.
  If a Veteran refuses to accept an eScreening tablet or is otherwise unable to do so, nurses and healthcare providers should conduct clinical reminder collection by standard protocol.

8.0 Risks and Mitigations

- Does the site have the necessary server configuration? Review 5.3 – 5.8 in this document for specifications.
- If the VistA version changes and the underlying RPC changes, MHE will have to be updated to reflect the updated Vista RPC calls.
- If using iPad mobile devices, refer to *IOS Risk Based Decision Memorandum* in the Appendix.

Appendix A – OIS Risk Based Decision Memo



OIS RBD 540 - Mental Health eScreening Assessment AC-11 IA-5 - CONDITIONAL APPROVED - 01-30-2015.pdf - Adobe Reader

File Edit View Window Help

Open | 1 / 4 | 81.4% | Tools | Fill & Sign | Comment

OIS RBD 540

Department of Veterans Affairs

OIS Risk Based Decision Memorandum

Date: JAN 30 2015

From: VHA 10P2D Innovations

Subj: Risk Mitigation Decision Regarding AC-11 and IA-5

To: Deputy Assistant Secretary, Information Security

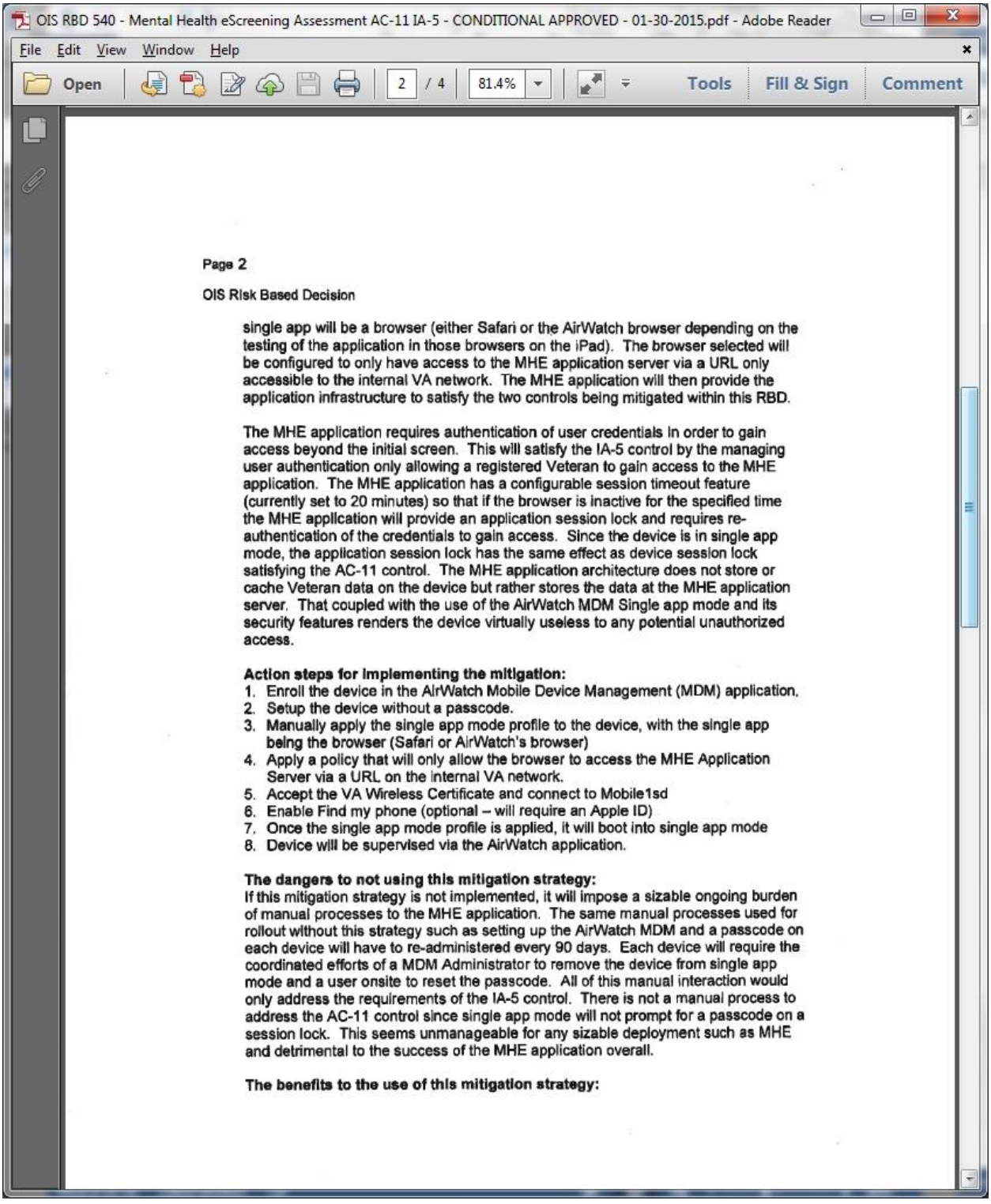
1. This document is ~~a local~~ an OIS risk based decision associated with the following VA Handbook 6500 Attachment 3 requirement: AC-11 Session Lock and VA Handbook 6500 Attachment 2 requirement: IA-5 Authenticator Management.

2. The recommended DISA STIG value found in Apple iOS 7 STIG Version 1 Release 1 and similarly found in the OIT AC-11 control is to set the maximum allotted session lock time to 15 minutes. This value cannot be used on this system because the Mental Health eScreening Assessment (MHE) iPad mobile devices must run in single app mode which never locks the device and does not prompt a user to reenter a password to unlock the device. Inherent to single app mode is the securing of the device to a single application which disables the device session lock feature built into the iPad. This is a limitation on Apple and how the single app mode functions. In single app mode there is no way to make the device prompt for a passcode upon wake up.

3. The recommended OIT value for the IA-5 control is for authenticators, such as a user password/passcode, to be changed every 90 days. This value cannot be used on this system because the Mental Health eScreening Assessment (MHE) iPad mobile devices must run in single app mode which does not allow a prompt for a passcode reset on the device. This is a physical limitation to the iPad hardware in single app mode and the only way to enable the passcode prompt is to remove the device from single app mode, which would provide open access to all apps on the device and is prohibitive.

4. I have determined that the appropriate mitigation strategy is to utilize the following safeguards to address the session lock and password/passcode controls. This Risk Based Decision memo and the mitigations are to be implemented and maintained throughout the life of the MHE application.

   We will employ the AirWatch Mobile Device Management (MDM) application in single app mode to lock down the iPad so that only one app can run on the device. This



single app will be a browser (either Safari or the AirWatch browser depending on the testing of the application in those browsers on the iPad). The browser selected will be configured to only have access to the MHE application server via a URL only accessible to the internal VA network. The MHE application will then provide the application infrastructure to satisfy the two controls being mitigated within this RBD.

The MHE application requires authentication of user credentials in order to gain access beyond the initial screen. This will satisfy the IA-5 control by the managing user authentication only allowing a registered Veteran to gain access to the MHE application. The MHE application has a configurable session timeout feature (currently set to 20 minutes) so that if the browser is inactive for the specified time the MHE application will provide an application session lock and requires re-authentication of the credentials to gain access. Since the device is in single app mode, the application session lock has the same effect as device session lock satisfying the AC-11 control. The MHE application architecture does not store or cache Veteran data on the device but rather stores the data at the MHE application server. That coupled with the use of the AirWatch MDM Single app mode and its security features renders the device virtually useless to any potential unauthorized access.

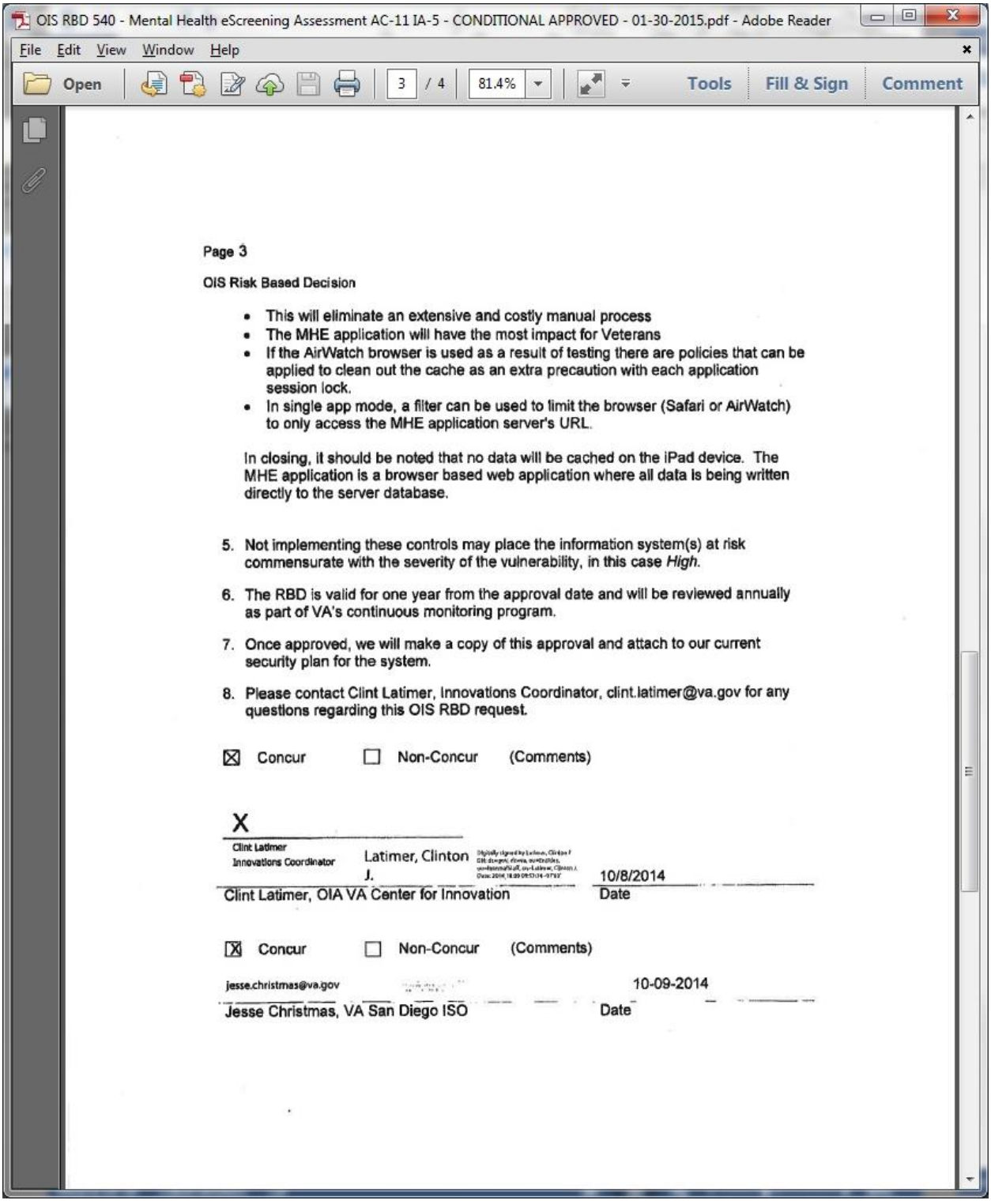
Action steps for implementing the mitigation:

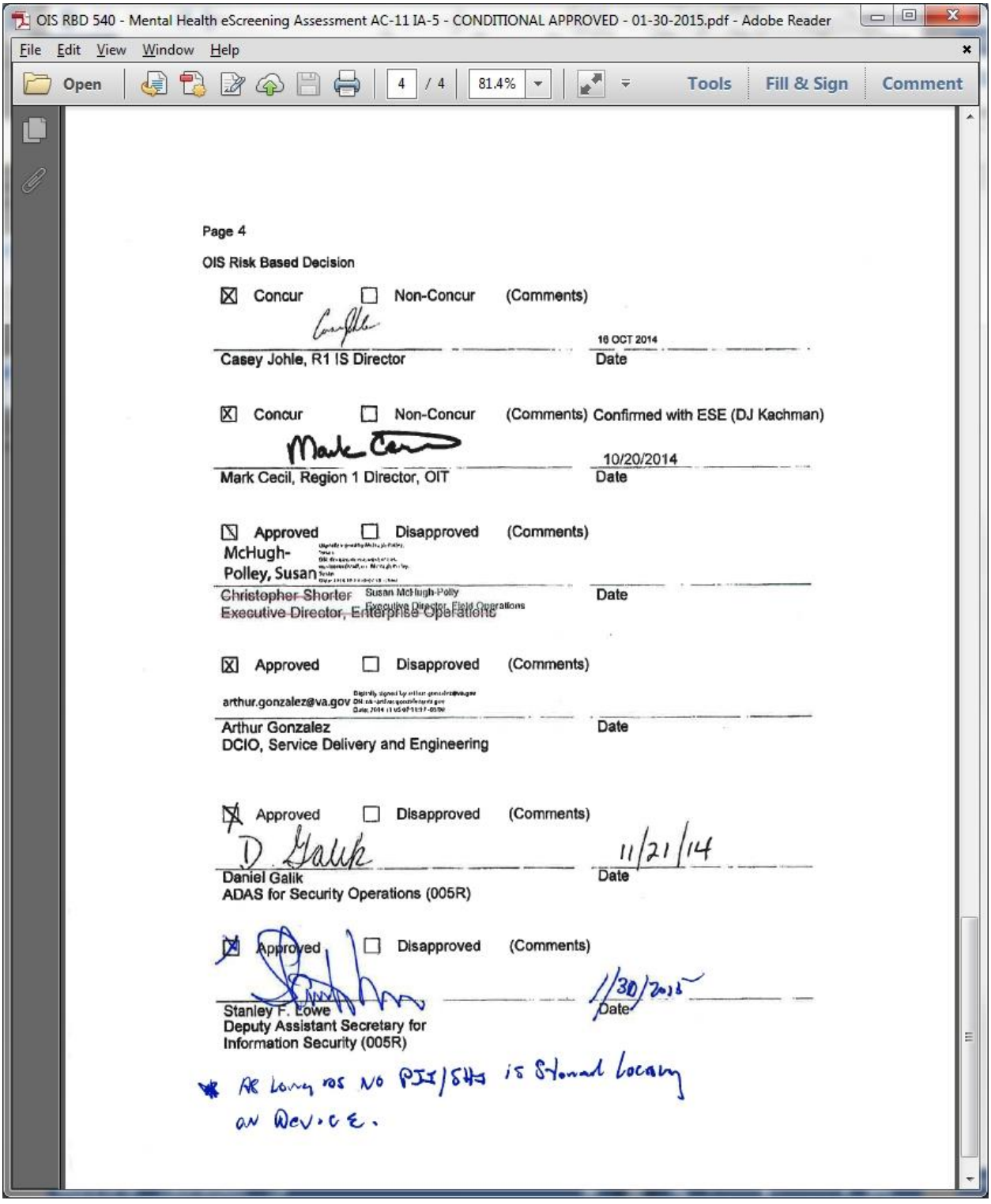
1. Enroll the device in the AirWatch Mobile Device Management (MDM) application.
2. Setup the device without a passcode.
3. Manually apply the single app mode profile to the device, with the single app being the browser (Safari or AirWatch's browser)
4. Apply a policy that will only allow the browser to access the MHE Application Server via a URL on the internal VA network.
5. Accept the VA Wireless Certificate and connect to Mobile1sd
6. Enable Find my phone (optional – will require an Apple ID)
7. Once the single app mode profile is applied, it will boot into single app mode
8. Device will be supervised via the AirWatch application.

The dangers to not using this mitigation strategy:

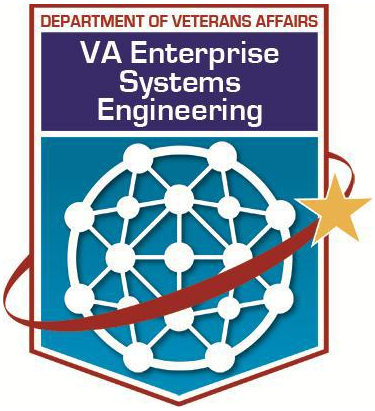
If this mitigation strategy is not implemented, it will impose a sizable ongoing burden of manual processes to the MHE application. The same manual processes used for rollout without this strategy such as setting up the AirWatch MDM and a passcode on each device will have to re-administered every 90 days. Each device will require the coordinated efforts of a MDM Administrator to remove the device from single app mode and a user onsite to reset the passcode. All of this manual interaction would only address the requirements of the IA-5 control. There is not a manual process to address the AC-11 control since single app mode will not prompt for a passcode on a session lock. This seems unmanageable for any sizable deployment such as MHE and detrimental to the success of the MHE application overall.

The benefits to the use of this mitigation strategy:


OIS RBD 540 - Mental Health eScreening Assessment AC-11 IA-5 - CONDITIONAL APPROVED - 01-30-2015.pdf - Adobe Reader
File Edit View Window Help
Open
3 / 4
81.4%
Tools
Fill & Sign
Comment
Page 3
OIS Risk Based Decision
This will eliminate an extensive and costly manual process
The MHE application will have the most impact for Veterans
If the AirWatch browser is used as a result of testing there are policies that can be applied to clean out the cache as an extra precaution with each application session lock.
In single app mode, a filter can be used to limit the browser (Safari or AirWatch) to only access the MHE application server's URL.
In closing, it should be noted that no data will be cached on the iPad device. The MHE application is a browser based web application where all data is being written directly to the server database.
5. Not implementing these controls may place the information system(s) at risk commensurate with the severity of the vulnerability, in this case High.
6. The RBD is valid for one year from the approval date and will be reviewed annually as part of VA's continuous monitoring program.
7. Once approved, we will make a copy of this approval and attach to our current security plan for the system.
8. Please contact Clint Latimer, Innovations Coordinator, clint.latimer@va.gov for any questions regarding this OIS RBD request.
☒ Concur ☐ Non-Concur (Comments)
X
Clint Latimer
Innovations Coordinator
Latimer, Clinton J.
10/8/2014
Clint Latimer, OIA VA Center for Innovation
Date
☒ Concur ☐ Non-Concur (Comments)
jesse.christmas@va.gov
10-09-2014
Jesse Christmas, VA San Diego ISO
Date


OIS RBD 540 - Mental Health eScreening Assessment AC-11 IA-5 - CONDITIONAL APPROVED - 01-30-2015.pdf - Adobe Reader
File Edit View Window Help
Open
4 / 4
81.4%
Tools
Fill & Sign
Comment
Page 4
OIS Risk Based Decision
☒ Concur ☐ Non-Concur (Comments)
Casey Johle, R1 IS Director
16 OCT 2014
Date
☒ Concur ☐ Non-Concur (Comments) Confirmed with ESE (DJ Kachman)
Mark Cecil, Region 1 Director, OIT
10/20/2014
Date
☒ Approved ☐ Disapproved (Comments)
McHugh-Polley, Susan
Christopher Shorter
Executive Director, Enterprise Operations
Susan McHugh-Polly
Executive Director, Field Operations
Date
☒ Approved ☐ Disapproved (Comments)
arthur.gonzalez@va.gov
Arthur Gonzalez
DCIO, Service Delivery and Engineering
Date
☒ Approved ☐ Disapproved (Comments)
D. Galik
Daniel Galik
ADAS for Security Operations (005R)
11/21/14
Date
☒ Approved ☐ Disapproved (Comments)
Stanley F. Lowe
Deputy Assistant Secretary for
Information Security (005R)
1/30/2015
Date
* As long as NO PII/SHI is Stored locally on Device.

Appendix B – VA OI&T Mobile Device Management



OFFICE OF INFORMATION AND TECHNOLOGY
ENTERPRISE SYSTEM ENGINEERING
CLIENT SERVICESMOBILE DIVISION

MDM Steps Start to Finish

Note: This document references numerous individual documents. All documentation can be found in the Mobile Documentation folder on the VA's Mobile Technologies SharePoint site.

Important! Only approved devices are authorized to be procured. **Do not procure or activate any VA non-approved devices.**

The current list of approved devices and apps are located at: *Approved Devices and Apps*
The list of approved apps is also located in this folder. Additionally, once Airwatch is installed, all approved VA applications will be available on the device home page under the icon "VA App Catalog". IT staff should go here to install VA approved applications to the device.

1. Local IT staff requests device from their procurement team and management chain.

2. Local IT staff receive device and complete required inventory steps (AMS/MERS)
    a. Device received by IT staff
    b. Device is entered or verified in inventory
    c. All assets are to be bar-coded and added to AEMS/MERS prior to deployment.
    The correct Category Stock Number (CSN) assignment for mobile devices and tablets include:
        - 7021-440001 COMPUTER, DIGITAL (Handheld/Palmtop/Blackberry)
        - 7021-440002 COMPUTER, DIGITAL (Laptop/Notebook) and Equipment Category of COMPUTER-TABLET
    d. Asset tag placed on the device
3. Local IT staff requests user and device enrollment into Airwatch from Region team.
    a. Contact information for regional admins located at: *MDM Regional Admins*
    Information to submit to regional admins:
        i. Active directory account name of user – i.e. vhawpbxxxxxx
        ii. Device EE number – 548EE12345
4. Region/VISN admin checks Airwatch to see if user is enrolled already
    a. If no, then Region adds user to Airwatch
    b. Document for Regional admins to add user and device is located at: *Adding User and Device in Airwatch*

5. Region admin adds device to user in Airwatch console
    a. Regional staff asked for inventory number when enrolling the device.

6. Reminder: Region admin and IT staff verify whether this user or device was previously set up with GOOD for email. There are different instructions below based on the whether the current user or device has GOOD for email. If the device currently has GOOD installed, then a few different steps MUST be done. These steps are noted below.

7. Region admin contacts local IT staff when the device is ready for provisioning

8. Local IT staff will configure the device with proper name and WLAN hotspot

a. Device is powered on and configured with the user account and VA naming conventions below. Documentation for new devices are located at: *Configuring a new iOS device*

b. Ensure that the device is configured with proper naming convention. **This step must be done by the local IT staff and is very important**. The device needs to be manually named properly prior to configuring Airwatch. VA naming policy can be found at:
Mobile Devices Naming Requirements

i. Open Settings – General – About – Name

ii. Change the name of the device to match the VA naming policy

c. Configure device to local IT wireless network (Hotspot for initial configuration, then Airwatch can push certificate for Cisco networks)

9. Airwatch application is installed and configured by the local IT staff - **Please note!** *There are different instructions based on the whether the current user has GOOD for email.*

a. The instructions below instruct you to install the Airwatch application from the application store. When downloading free Airwatch app, IT staff can create an Itunes or Google Play account for user's device. Instructions for creating free accounts are located at:

i. Apple Itunes: Create an Apple ID without credit card

ii. Google play: Create Google Play ID without credit card

b. Choose the correct installation instructions based on the user or device situation:

i. Instructions for installing and configuring Airwatch on a **new device** for a user **NOT already enrolled with the GOOD email program** are located at: Activating Device with Airwatch

ii. Instructions for installing and configuring Airwatch on a **device that already has GOOD** or for a **user that has been using GOOD** are located at: Remove GOOD install Airwatch MDM

Please note that you will have to remove a GOOD profile AND/OR contact your Regional MDM admin to request a change to the user's GOOD profile. *If you do not follow these steps correctly, you will have two programs that will conflict, resulting in a longer troubleshooting process!*

c. Once Airwatch is installed, IT staff with run the Airwatch app

d. Device is enrolled into Airwatch through the Airwatch application with the information emailed by Regional admin.

10. IT staff might need to configure the device to a permanent wireless network.

a. If the device needs to connect to the VA Cisco certificate based wireless network, the Local IT staff will request from Regional MDM Admin a manual push of the certificate. After this certificate is installed, then local IT staff can configure the device to the new network and instruct the device to "forget" the public network. Instructions are at*: Install National Wireless Certificate to Device Using Airwatch*

11. If user will need email (or is currently using GOOD for email), then Region admin requests GOOD account from the Mobile team. (Contact the NSD, open a Remedy Ticket for user to be added to Good.)

Very important! Prior to opening the GOOD application, if user already has GOOD, Mobile team will have to transition from GOOD MDM to GOOD with Airwatch. Contact your Regional MDM Admin and request the user's GOOD profile to be changed. *Failure to do this will result in additional work due to conflicting profiles on the device.*

b. If user is allowed access to email on device, GOOD application must be installed and configured. All approved VA applications will be available on the device home page under the icon "VA App Catalog". IT staff should go here to install applications such as Citrix receiver or GOOD for email

c. Install GOOD and Configure GOOD (see *GOOD iPhone Quickstart*)

12. If the user or device is approved for Citrix receiver, the local IT staff will install from the VA app catalog.

13. All approved VA applications will be available on the device home page under the icon "VA App Catalog". IT staff should go here to install applications such as Citrix receiver or GOOD for email
a. Instructions for how to configure Citrix are at: *iOS Citrix Client Setup Configuration*

14. The Regional admin will verify that the device has successfully enrolled into the Airwatch console. Once this is done, they will inform the Local IT staff that the device is enrolled

15. Before turning the device over to the user, the Local IT staff will
    a. Open the Airwatch application on the device
    b. Verify that the Status reads as "Device Enrolled"

16. User is properly trained on device and signs rules of behavior. User is emailed or handed *Mobile Device Tips GFE*. This document outlines their responsibilities regarding these devices.

17. Airwatch Check-in every 48 hours. The user will have to check in with Airwatch every 2 days. This is done by opening the Airwatch app, waiting for it to load, and then clicking the home button to return to the desktop. The process will take less than 3 seconds and is the only way for the device to communicate information properly to the server.

Appendix C - MHE Samsung Tablet Security Steps

Note: Log-in user IDs and passwords are subject to change. These are current in March 2015.

Admin log-in

User: vhasdc….
Pass: (not supplied)

eScreening log-in

User: .\vhasdescreen
Pass: Escreen#1

Contents

MHE SAMSUNG TABLET SECURITY STEPS 43

1) Change the View for the Assessment 43
2) Download Keycall off of R Drive 43
3) Add Printer to the Tablet 43
4) Authorizing VHASDCESCREEN to Have Administrator's Rights 43
5) Prevent Microsoft Lync from Launching at Startup. 43
6) Install Mozilla Firefox 29.0 43
7) Disable Access to IE 44
8) Unpining All Icons (Except Firefox) on the Task bar 44
9) Make Firefox Open on Startup 44
10) Changing On-Screen Keyboard Settings 44
11) Installing Custom On-Screen Keyboard 44
12) Installing Add-Ons for Firefox Interface 45
13) Removing Desktop Items 45
14) Locking & Removing All Settings 45
15) Revoking VHASDCESCREEN Administrator's rights 46
16) Test Locked Down Tablet 46

STEP-BY-STEP SCREENSHOTS 48

1) Change the View for the Assessment 48
2) Download Keycall off of R Drive 48
3) Add Printer to the Tablet 50
4) Authorizing VHASDCESCREEN to Have Administrator's Rights 51
5) Prevent Microsoft Lync from Launching at Startup. 51
6) Install Mozilla Firefox 29.0 51
7) Disable Access to IE 53
8) Unpinning All Icons (Except Firefox) on the Task bar 54
9) Make Firefox Open on Startup 54
10) Changing On-Screen Keyboard Settings 57
11) Installing Custom On-Screen Keyboard 59
12) Installing Add-Ons for Firefox Interface 61
13) Removing Desktop Items 65
14) Locking & Removing All Settings 66

15) REVOKING VHASDCESCREEN ADMINISTRATOR'S RIGHTS 71
16) PERFORM THE FINAL LOCKDOWN STEP. 73
17) TEST LOCKED DOWN TABLET 75

SAMSUNG TABLETS MAINTENANCE & TROUBLESHOOTING STEP-BY-STEP GUIDE 76

REAUTHORIZE VHASDCESCREEN TO HAVE ADMINISTRATOR'S RIGHTS 76
BACKDOOR TO GPEDIT WHEN SEARCH DISABLED 76
STARTUP FOLDER NOT SHOWING UP IN ALL PROGRAMS LIST 78
CANNOT ADD SHORTCUT IN STARTUP FOLDER 79
RIGHT-CLICKING DOES NOT DO ANYTHING (NO CONTEXT MENUS AVAILABLE) 80
KEYCALL ERROR MESSAGE UPON INSTALLATION 80

MHE Samsung Tablet Security Steps

1) Change the View for the Assessment

a) Login as Mhe admin user
b) Right-Click in any empty space on the desktop and select **Screen Resolution**
c) Change the orientation from landscape to portrait (or **ctrl+alt+"up arrow"**)
d) Click **OK**

2) Download Keycall off of R Drive

a) **My H Drive → Afari – Shortcut → eScreening Expansion 2014 → hardware**
b) Drag-and-drop **Keycall** folder to **Public Documents** library **(**hover over **Documents** library → **copy to Public Documents) → OK**
c) Close all open folders

3) Add Printer to the Tablet

a) **Start → Run** (or type "**Run**" → **Enter**
b) Type \\vhasdcfpc1\SDC-PT01-1587P1 → **OK**

4) Authorizing VHASDCESCREEN to Have Administrator's Rights

a) Open Control Panel. Under **User Accounts**, select **Change account type**. Then select **VHASDCESCREEN**, then click **Properties**
b) Under Group Membership, select **Administrator**
c) Click **OK** and log off, then log in as **VHASDCESCREEN**

5) Prevent Microsoft Lync from Launching at Startup.

a) Go to **Options**, click **Personal,** and uncheck **Automatically start Lync when I log on to Windows**

6) Install Mozilla Firefox 29.0

a) Open **Internet Explorer**
b) Google Firefox (**MAKE SURE YOU ARE DOWNLOADING FROM THE MOZILLA WEBSITE) →** click **Free Download → Run**
c) **Options →** Uncheck the option to install automatic update service. **→ Install**
d) In the **Firefox** window, open **Menu** and select **Options**
e) Under General, type the MHE Website URL as the homepage
f) Under Security, uncheck **Remember passwords for sites**
g) Under Advanced and under the Update tab, select **Never check for updates**
h) Click **OK**
i) Right-click Firefox icon on taskbar **→ Pin this program to taskbar**

7) Disable Access to IE

a) Go to **Start** and open **Default Programs**
b) Select **Set program access and computer defaults**
c) Under **Custom**, click the list, then select **Firefox** as default web browser
d) Disable access to IE

8) Unpinning All Icons (Except Firefox) on the Task bar

a) Right-click each icon and select **unpin**

9) Make Firefox Open on Startup

a) Go to **Start → All Programs →** right-click the **Startup** folder **→ Open all Users**
b) Right-Click inside the folder **→ New →Shortcut**
c) Browse to:
   Computer > C: > Program Files > Mozilla Firefox > Firefox.exe
d) Select and click **OK**
e) Click **Next**, then click **Finish**

10) Changing On-Screen Keyboard Settings

a) Bring up the on-screen keyboard by touching the left edge of the screen
b) Click **Tools → Docking → Dock at bottom of screen**
c) Click **Tools → Options**
d) Under the **Opening** tab, uncheck all settings except **For tablet pen input, show icon next to the text box**
e) Click **OK**

NOTE: You must have a mouse and keyboard installed to continue

11) Installing Custom On-Screen Keyboard

a) **Start → Documents → Keycall → AutoHotkey104805_install → Next → I Agree → Next → Install →** (Optional: deselect: **Show Readme**) **→ Finish**
b) In the **Keycall** folder, double-click the icon to open **keycall.ahk (Even though it does not look like it, something happened)**. Keep the folder open
c) Using a mouse, open **Start →** A**ll Programs**, then right click the **Startup** folder.
d) Choose **Open all users** (for convenience (& if you know how) "snap" the two windows (startup & Documents>keycall) on opposite sides of the screen)
e) Right-click on **keycall.ahk → Create shortcut**
f) Drag & Drop the **shortcut** to the **Startup** folder
g) Close both folders
h) Restart tablet, log back in, & test custom keyboard

12) Installing Add-Ons for Firefox Interface

a) Open **Firefox →Menu→Add-ons**
b) Search for & install the following add-ons:
   i) **Hide Tab Bar With One Tab (“**hide tab” search works)
   ii) **Hide Navigation Bar** (“hide navigation” search works)
   iii) **Hide Caption Titlebar Plus** (“hide caption” search works)
   iv) **Blocksite**
   v) **Blocksite → Restart now → I don’t want help**
c) **Menu→Add-ons → Extensions (**make sure all four are enabled)
   i) **Blocksite→Options**
      (1) Make sure **Whitelist** is selected
      (2) Click **Add →**add current Mhe URL **→ OK → OK** again
   ii) **Hide Caption → Options**
      (1) **Look & Feel** tab **→** select the following: Show Custom… “**Never**”; System borders “**Disabled**” and unselect **Activate custom borders…**; In Maximized and Un-Maximized window options “**Disabled**”; System Titlebar “**System Titlebar always hidden”**
      (2) **Look & Feel 2** tab **→** select the following: Options for Firefox… deselect “**Enable custom Firefox ‘Home’ Button**; Deselect “**Floating…**”; Full-Screen mode option select “**Autohide also Firefox…”**
      (3) Click **OK**
   iii) **Hide Navigation Bar → Options**
      (1) General tab **→** Select “**Enable Hide Navigation Bar**” & “**Hide the Navigation Bar**”
      (2) Auto-Hide tab **→** Select “**Enable Auto-Hide**”
      (3) Click **Apply → OK**
d) Close Firefox and reopen to test status → Firefox window should only show webpage

13) Removing Desktop Items

a) Right-click on the desktop and select **Personalize**
b) Click **Change desktop icons**
c) Uncheck all options
d) **Apply** and **Close**

14) Locking & Removing All Settings

a) **Start**
b) Search and open **gpedit.msc**, and **minimize (do not close)**
c) Search and open **cmd.exe**, and **minimize (do not close)**
d) Right-click **taskbar → properties**
   i) Taskbar tab **→** check both **Lock the taskbar** & **Auto-hide the taskbar**
   ii) Start Menu tab **→ Customize**
      (1) Uncheck everything and select **Don’t display this item** for everything (scroll up and down in the window to ensure that everything is deselected and not displayed)
      (2) **Apply** and **Close**
e) Maximize **the Local Group Policy Editor** window

i) Browse to User Configuration > Administrative Templates > Desktop
   (1) Open **Hide and disable all items on the desktop**, **Enable**, and click **OK**
ii) Browse to User Configuration > Administrative Templates > Start Menu and Taskbar (click the top "**Setting**" bar to alphabetize the options)
   (1) Open **Hide the notification area**, **Enable**, and click **OK**
   (2) Open **Lock all taskbar settings**, **Enable**, and click **OK**
   (3) Open **Lock the taskbar**, **Enable**, and click **OK**
   (4) Open **Prevent changes to taskbar and start menu settings**, **Enable**, and click **OK**
   (5) Open **Prevent users from adding or removing toolbars**, **Enable**, and click **OK**
   (6) Open **Remove All Programs list from the start menu**, **Enable**, and click **OK**
   (7) Open **Remove clock from the system notification area**, **Enable**, and click **OK**
   (8) Open **Remove common program groups from start menu**, **Enable**, and click **OK**
   (9) Open **Remove drag-and-drop and context menus from start menu**, **Enable**, and click **OK**
   (10) Open **Remove frequent programs list from start menu**, **Enable**, and click **OK**
   (11) Open **Turn off all balloon notifications**, **Enable**, and click **OK**
iii) Browse to User Configuration > Administrative Templates > System > Ctrl+Alt+Del Options
   (1) Open **Remove change password**, **Enable**, and click **OK**
   (2) Open **Remove task manager**, **Enable**, and click **OK**
iv) Browse to User Configuration > Administrative Templates > Control Panel
   (1) Open **Prohibit access to the control panel**, **Enable**, and click **OK**
v) Close **Local Group Policy Editor**

f) Maximize the **Command Prompt**
   i) Type **gpupdate /force** and press **Enter**

15) Revoking VHASDCESCREEN Administrator's rights

a) Type **lusrmgr** and press **Enter**
b) Open the **Users** folder
c) Right-Click **VHASDCESCREEN → Properties**
d) Under the **Member Of** tab **→ Administrators → Remove**
e) Click **Add** and type **Users → Check Names → OK**
f) Click **OK** again **→** close all windows

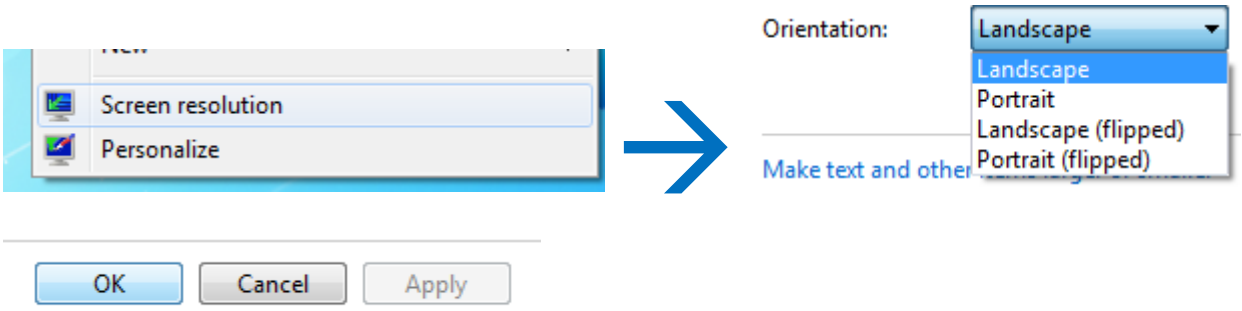
16) Test Locked Down Tablet

a) **Shut down** the tablet and turn it back on **(do not just Restart**. You need to determine if everything works as it is supposed to from a cold start**)**
b) Log in as **VHASDCESCREEN**
   i) The eScreening website should popup and there should be no: top "min/max/exit" bar, add tab bar, or address bar
   ii) Click Start eScreening
   iii) When you click in the two fields, the custom keyboard icon should appear
c) Close **Firefox**
   i) Move mouse to (or touch) the bottom of the screen
   ii) Right-click (or apply constant pressure to) the **Firefox** icon **→ Close window**
d) There should be nothing on the **Desktop or Taskbar**
e) Click the **Start** button, there should be no options besides the search bar

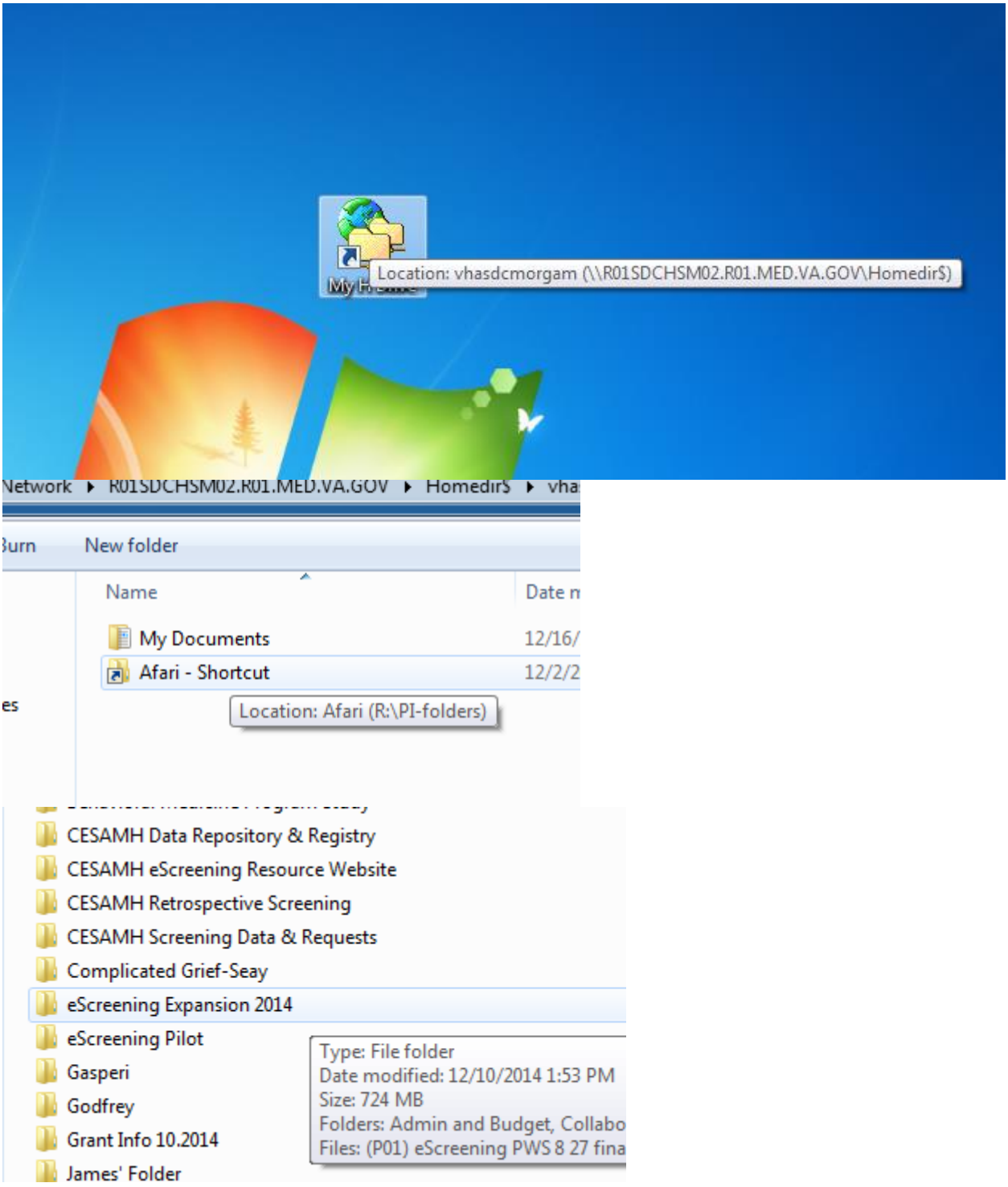
f) Try searching for something. It should display no results
g) If all of the previous points are true, the tablet is locked down correctly
h) If not, backtrack and try to determine what is not correct. Check the troubleshooting section further down for tips and tricks.

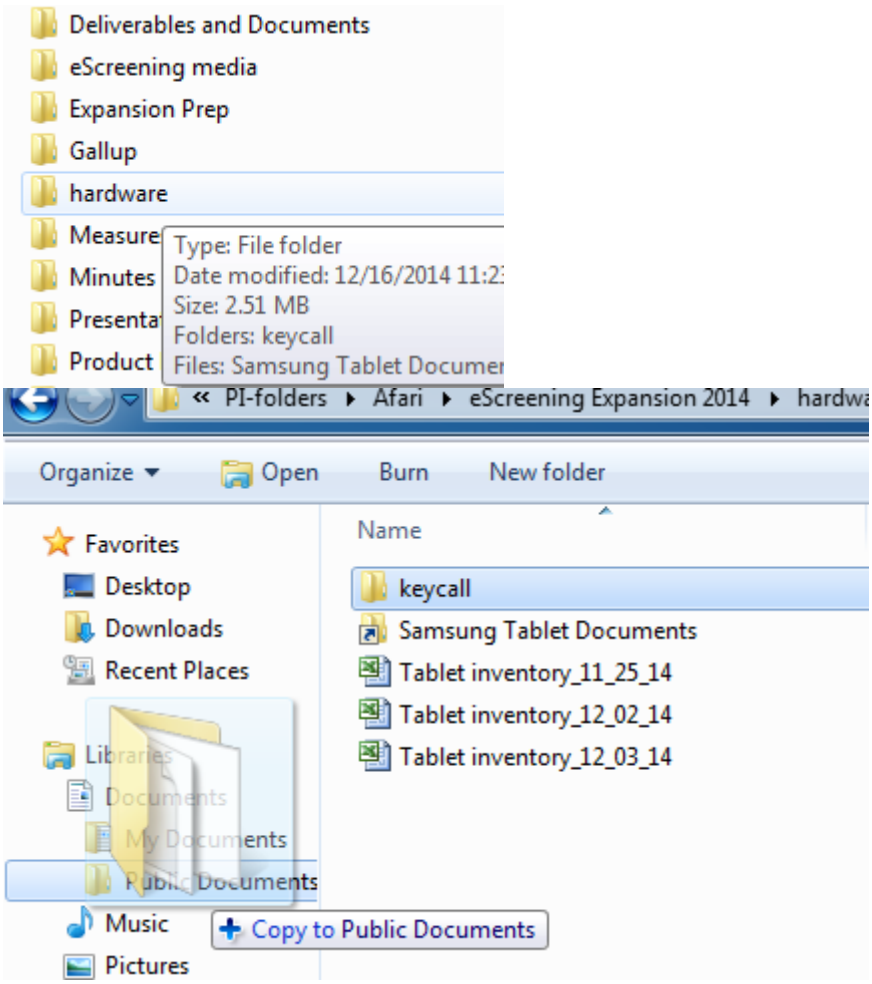
Step-by-Step with Screenshots

1) Change the View for the Assessment

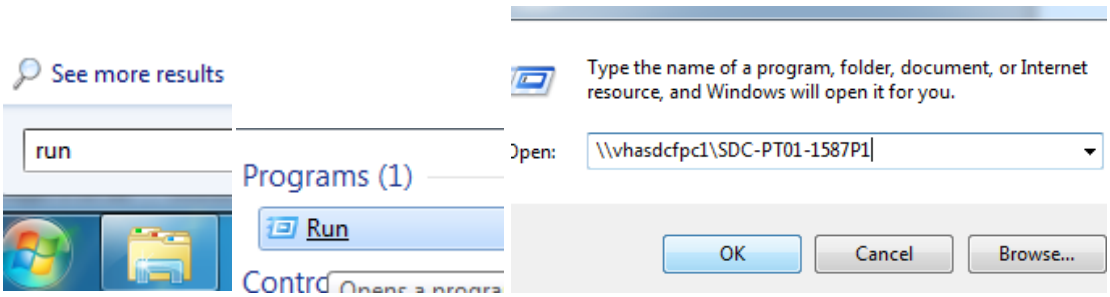


2) Download Keycall off of R Drive

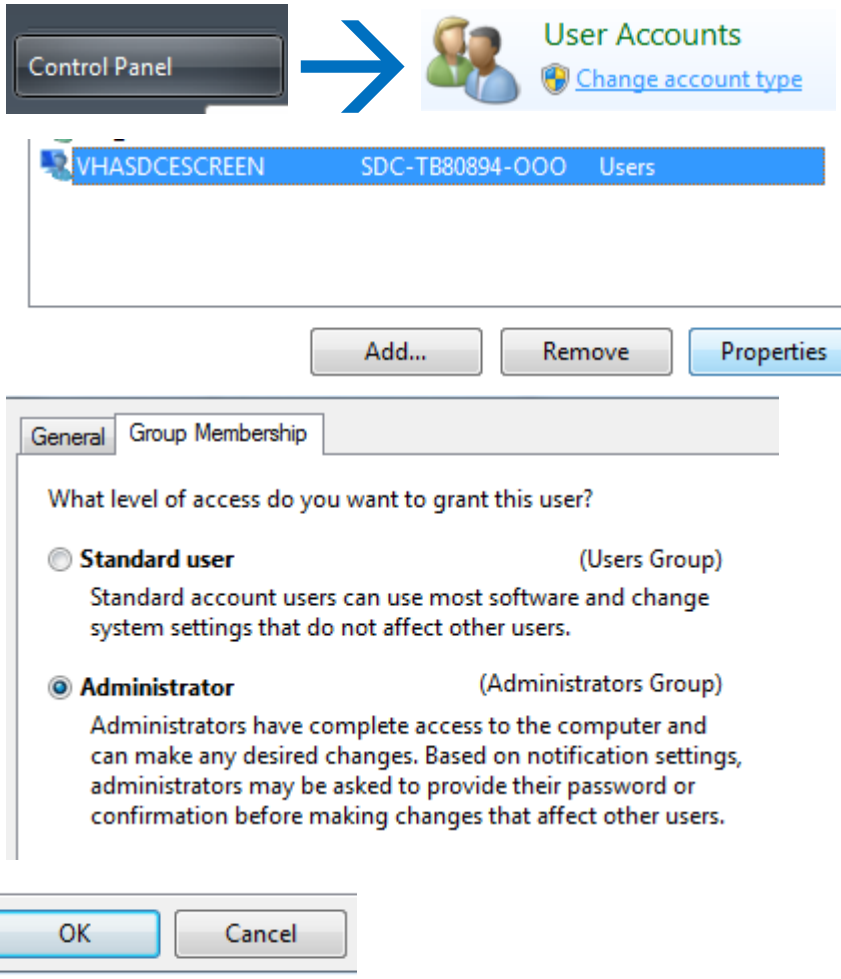

Location: vhasdcmorgam (\\R01SDCHSM02.R01.MED.VA.GOV\Homedir$)
Network ▸ R01SDCHSM02.R01.MED.VA.GOV ▸ Homedir$ ▸
Burn
New folder
Name
My Documents
Afari - Shortcut
Location: Afari (R:\PI-folders)
CESAMH Data Repository & Registry
CESAMH eScreening Resource Website
CESAMH Retrospective Screening
CESAMH Screening Data & Requests
Complicated Grief-Seay
eScreening Expansion 2014
eScreening Pilot
Gasperi
Godfrey
Grant Info 10.2014
James' Folder
Type: File folder
Date modified: 12/10/2014 1:53 PM
Size: 724 MB
Folders: Admin and Budget, Collabo
Files: (P01) eScreening PWS 8 27 fina



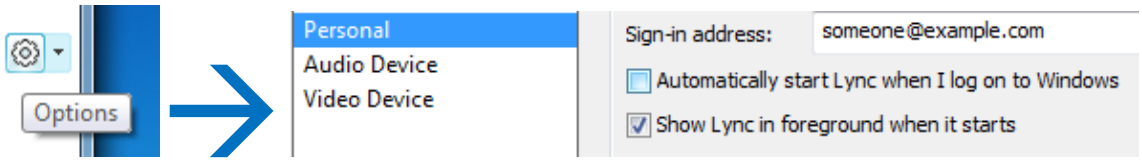
3) Add Printer to the Tablet



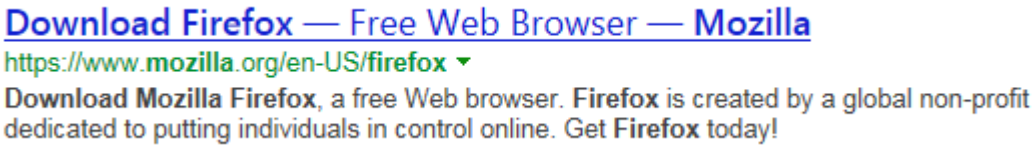
4) Authorizing VHASDCESCREEN to Have Administrator's Rights

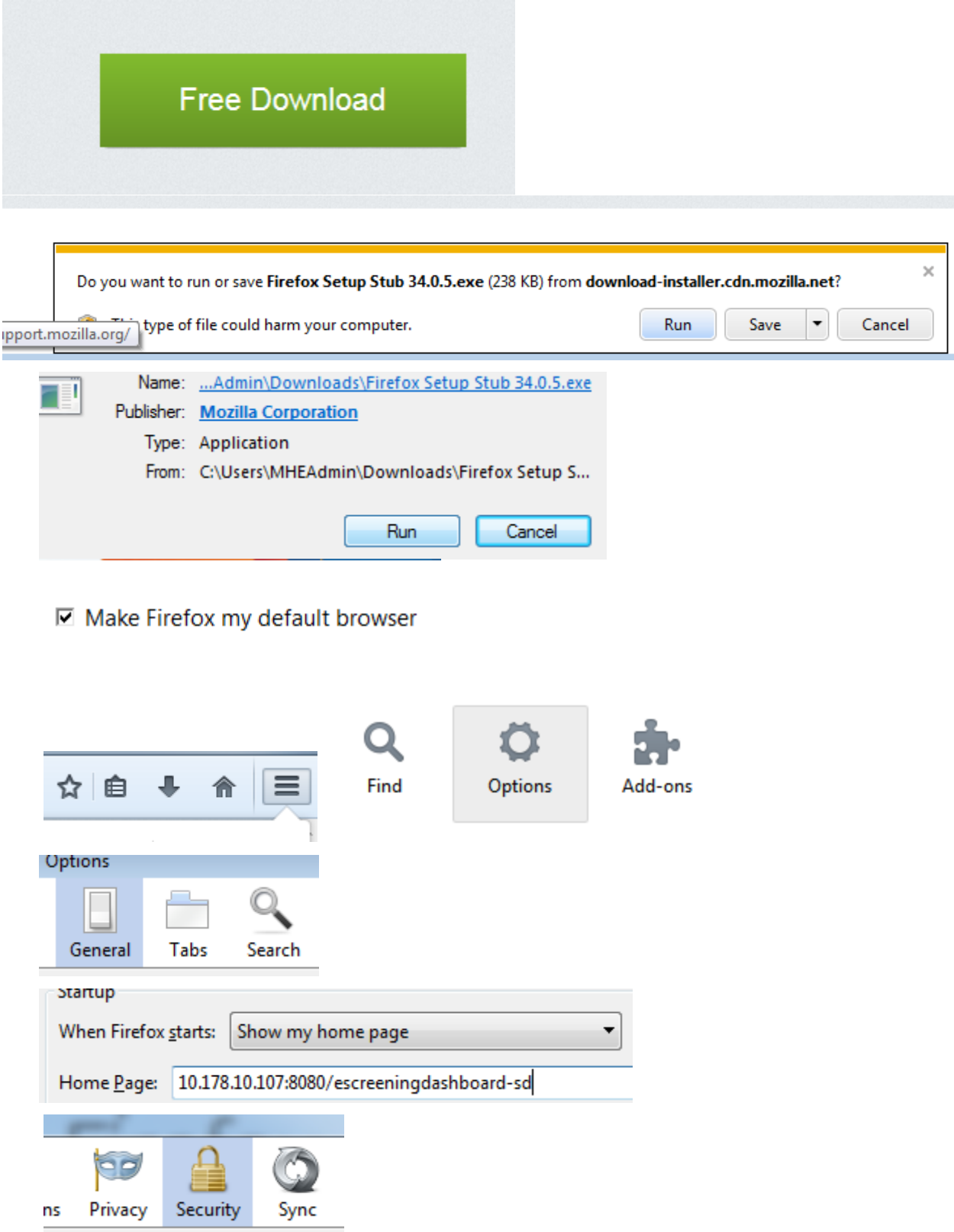


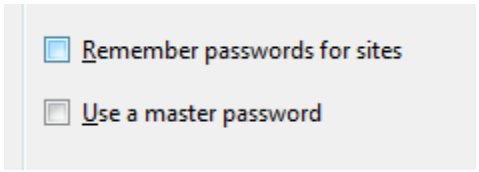
5) Prevent Microsoft Lync from Launching at Startup.

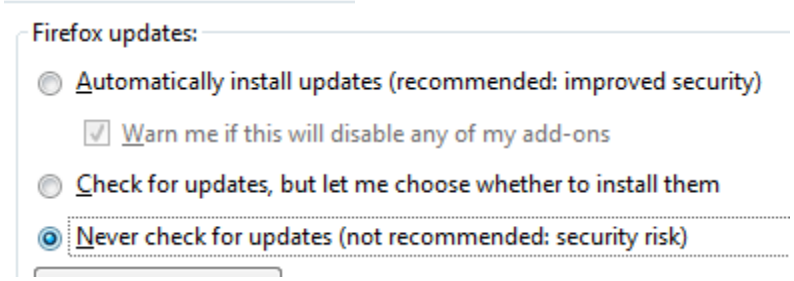


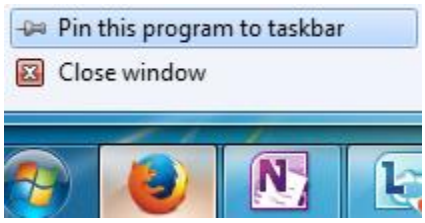
6) Install Mozilla Firefox 29.0



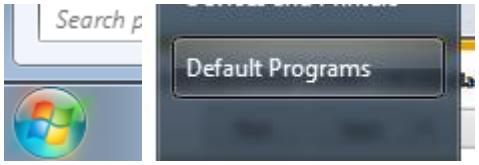

Free Download
Do you want to run or save Firefox Setup Stub 34.0.5.exe (238 KB) from download-installer.cdn.mozilla.net?
type of file could harm your computer.
Run
Save
Cancel
Name: ...Admin\Downloads\Firefox Setup Stub 34.0.5.exe
Publisher: Mozilla Corporation
Type: Application
From: C:\Users\MHEAdmin\Downloads\Firefox Setup S...
Run
Cancel
Make Firefox my default browser
Find
Options
Add-ons
Options
General
Tabs
Search
Startup
When Firefox starts:
Show my home page
Home Page:
10.178.10.107:8080/escreeningdashboard-sd
Privacy
Security
Sync

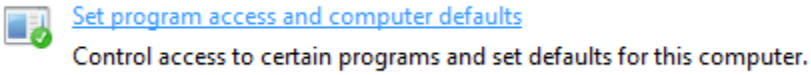


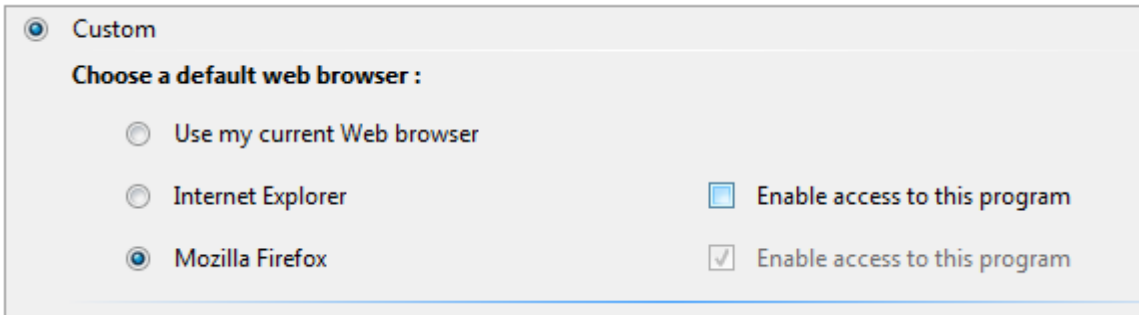




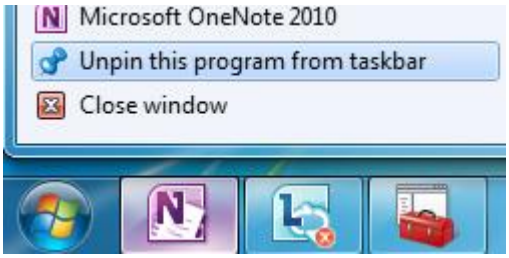
7) Disable Access to IE



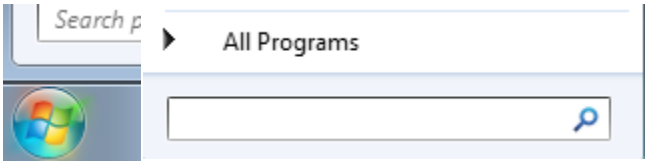


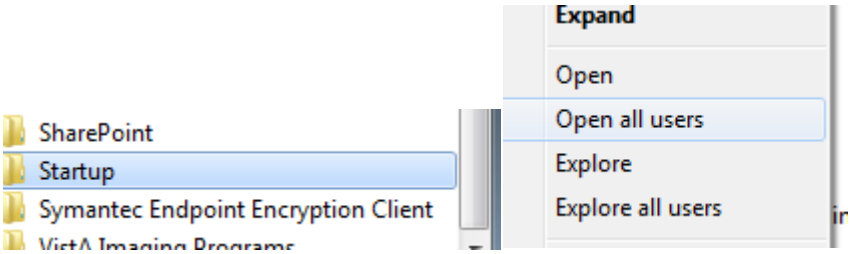


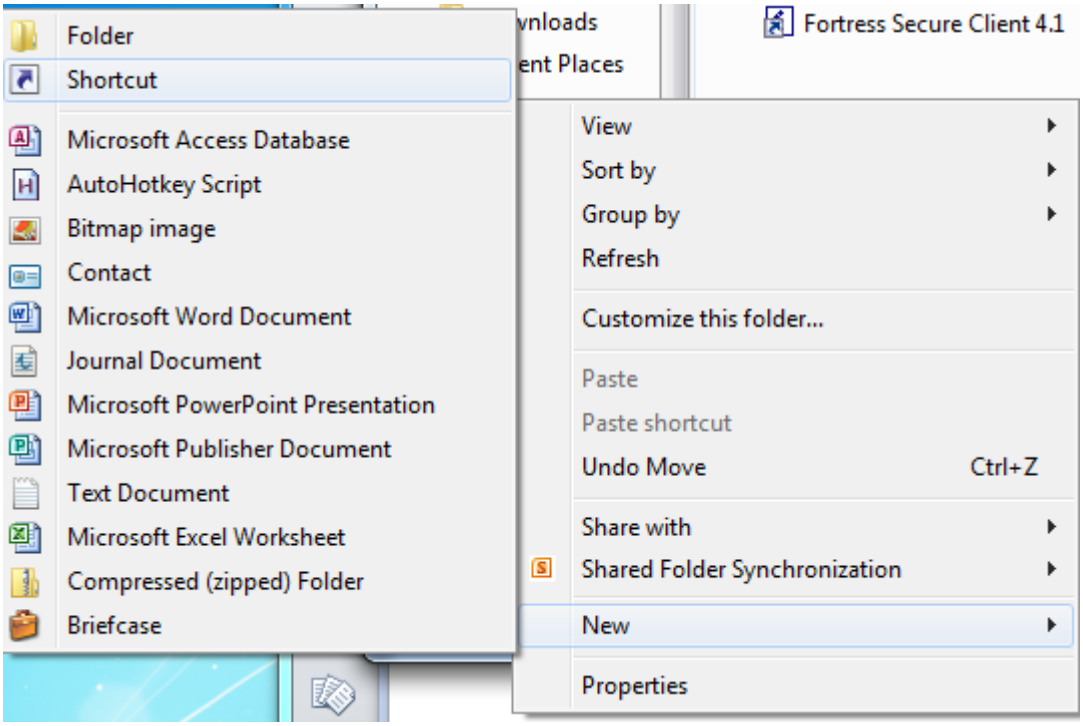
8) Unpinning All Icons (Except Firefox) on the Task bar



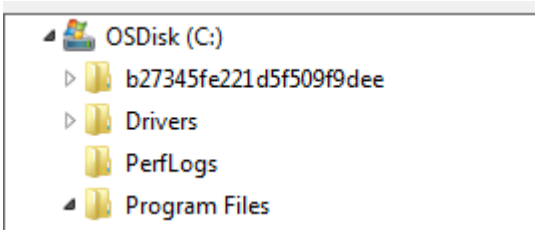
9) Make Firefox Open on Startup

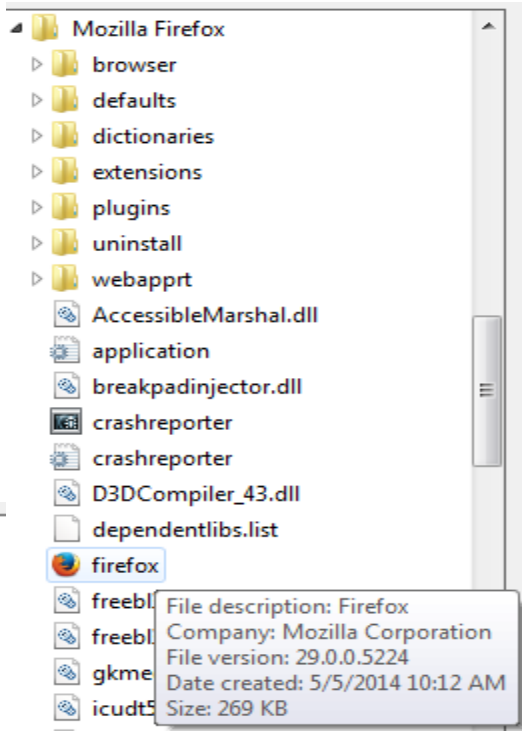


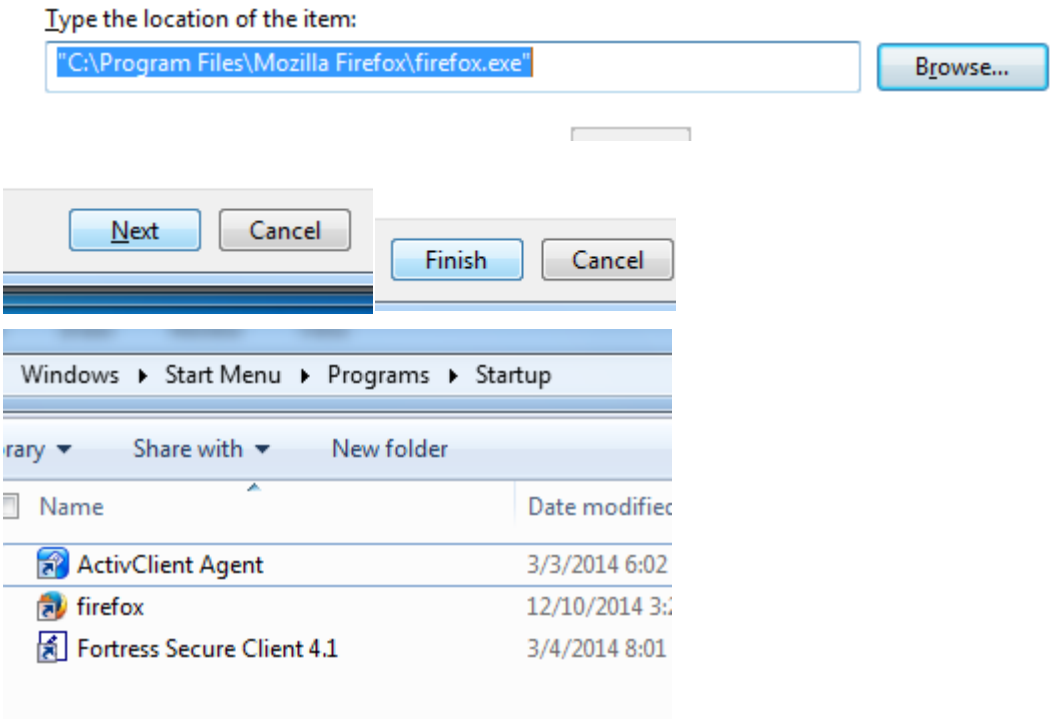



Folder
Shortcut
Microsoft Access Database
AutoHotkey Script
Bitmap image
Contact
Microsoft Word Document
Journal Document
Microsoft PowerPoint Presentation
Microsoft Publisher Document
Text Document
Microsoft Excel Worksheet
Compressed (zipped) Folder
Briefcase
Fortress Secure Client 4.1
View
Sort by
Group by
Refresh
Customize this folder...
Paste
Paste shortcut
Undo Move Ctrl+Z
Share with
Shared Folder Synchronization
New
Properties

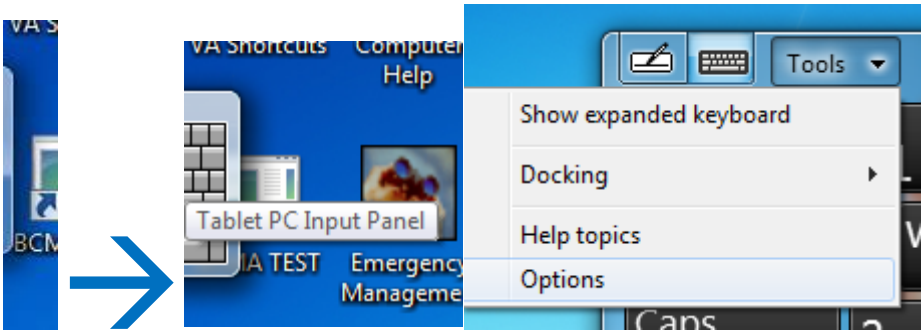
Browse...

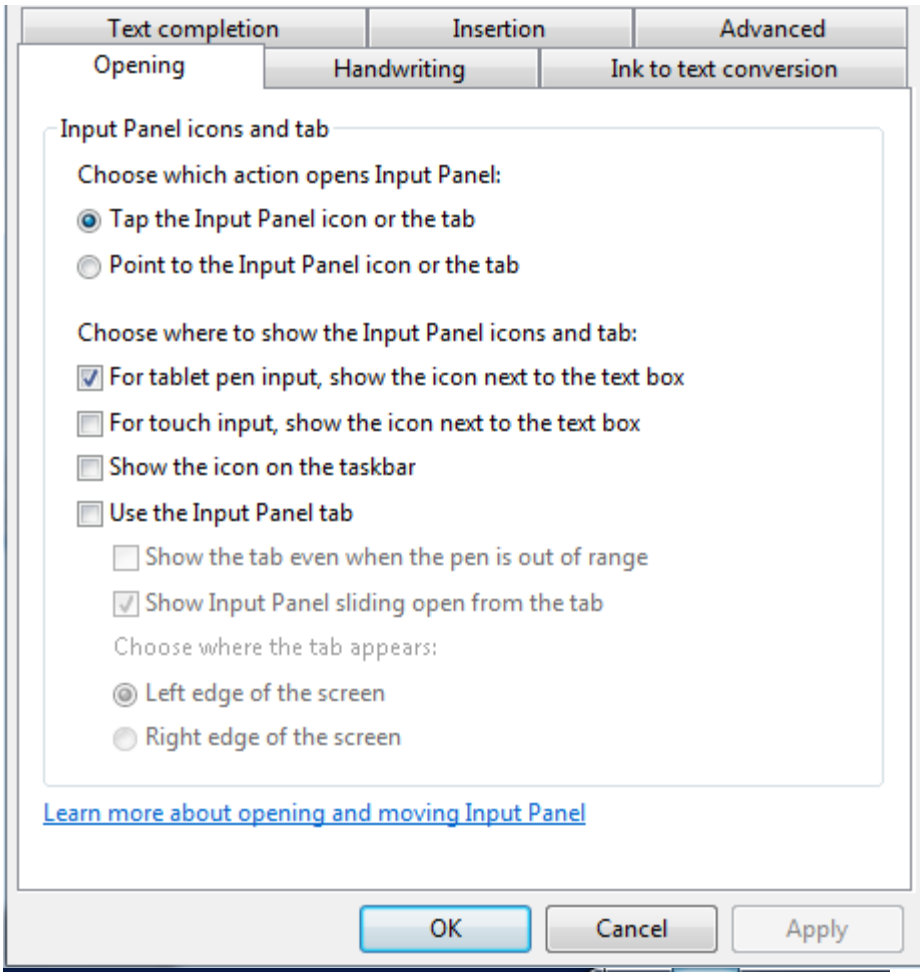

OSDisk (C:)
b27345fe221d5f509f9dee
Drivers
PerfLogs
Program Files

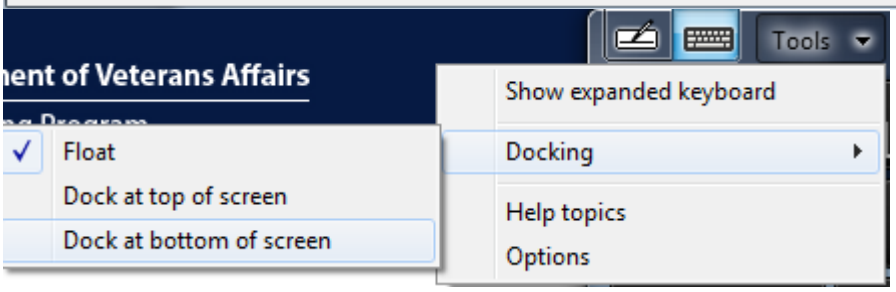

Mozilla Firefox
browser
defaults
dictionaries
extensions
plugins
uninstall
webapprt
AccessibleMarshal.dll
application
breakpadinjector.dll
crashreporter
crashreporter
D3DCompiler_43.dll
dependentlibs.list
firefox
File description: Firefox
Company: Mozilla Corporation
File version: 29.0.0.5224
Date created: 5/5/2014 10:12 AM
Size: 269 KB


Type the location of the item:
"C:\Program Files\Mozilla Firefox\firefox.exe"
Browse...
Next
Cancel
Finish
Cancel
Windows ▸ Start Menu ▸ Programs ▸ Startup
Share with
New folder
Name
Date modified
ActivClient Agent
3/3/2014 6:02
firefox
12/10/2014
Fortress Secure Client 4.1
3/4/2014 8:01

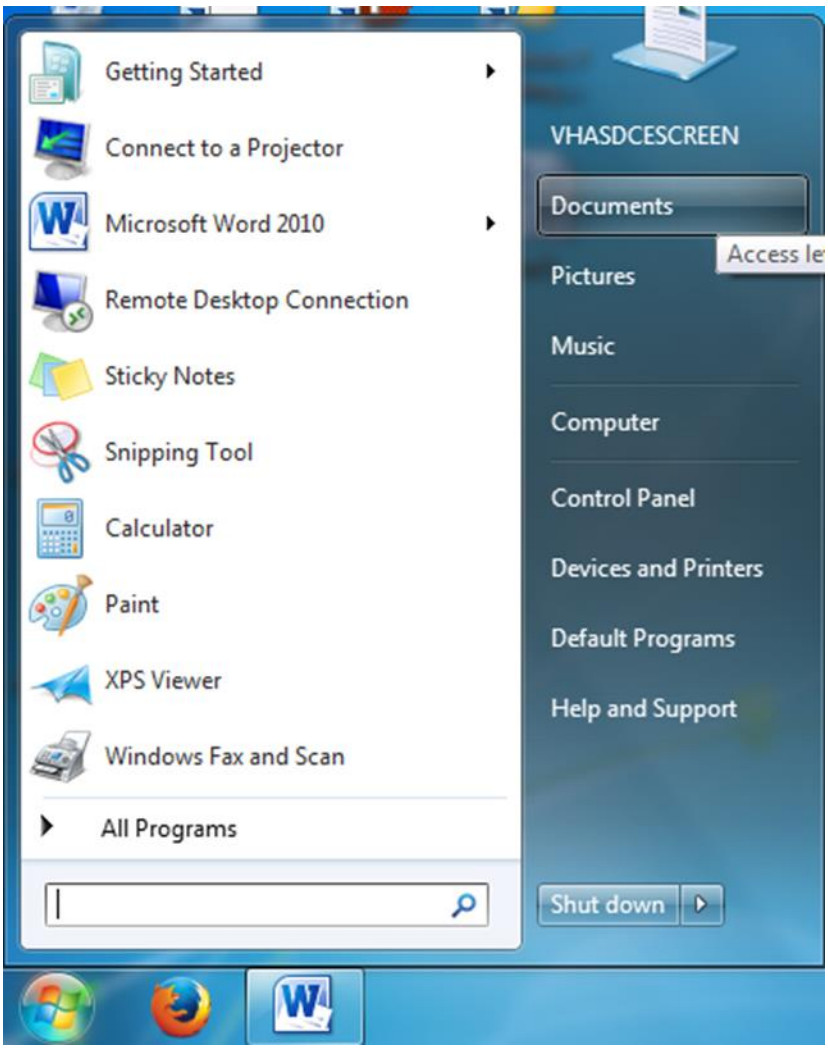
10) Changing On-Screen Keyboard Settings

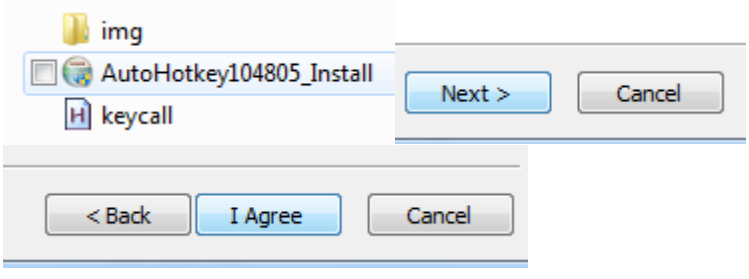

Tablet PC Input Panel
Tools
Show expanded keyboard
Docking
Help topics
Options

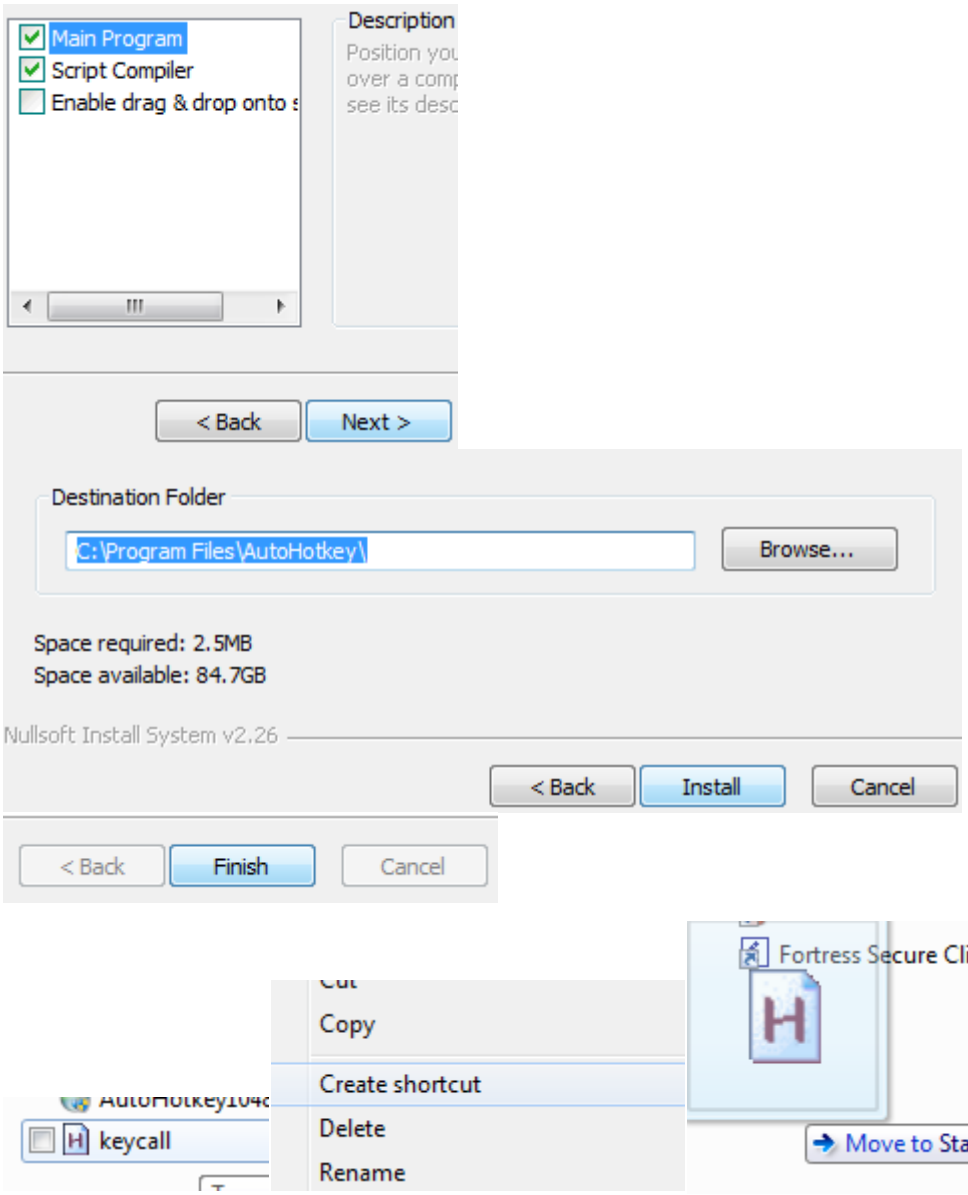

Text completion
Insertion
Advanced
Opening
Handwriting
Ink to text conversion
Input Panel icons and tab
Choose which action opens Input Panel:
Tap the Input Panel icon or the tab
Point to the Input Panel icon or the tab
Choose where to show the Input Panel icons and tab:
For tablet pen input, show the icon next to the text box
For touch input, show the icon next to the text box
Show the icon on the taskbar
Use the Input Panel tab
Show the tab even when the pen is out of range
Show Input Panel sliding open from the tab
Choose where the tab appears:
Left edge of the screen
Right edge of the screen
Learn more about opening and moving Input Panel
OK
Cancel
Apply

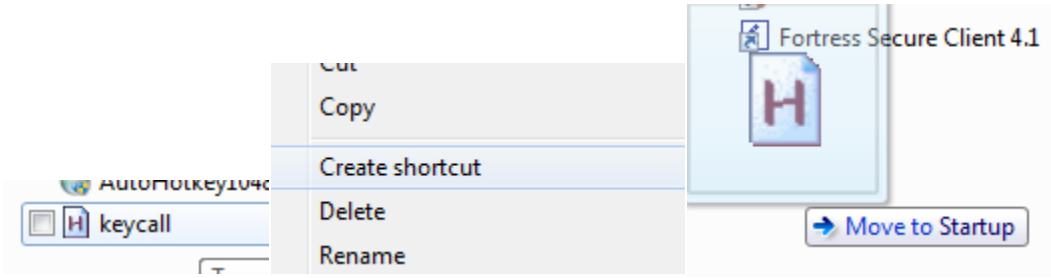

Tools
Show expanded keyboard
Float
Docking
Dock at top of screen
Dock at bottom of screen
Help topics
Options

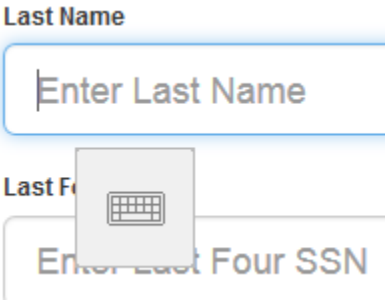
11) Installing Custom On-Screen Keyboard



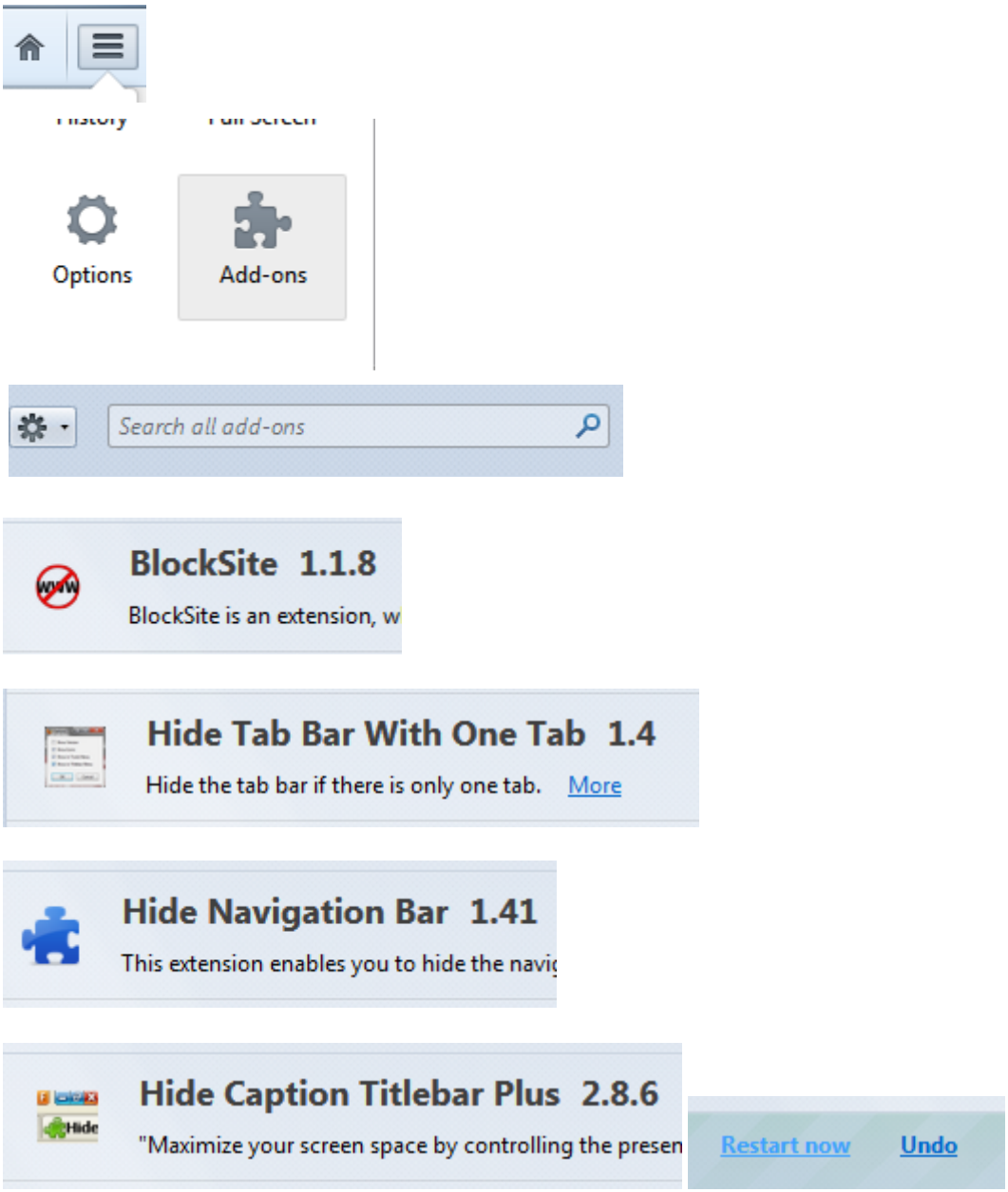



Main Program
Script Compiler
Enable drag & drop onto s
Description
Position you
over a comp
see its desc
< Back
Next >
Destination Folder
C:\Program Files\AutoHotkey\
Browse...
Space required: 2.5MB
Space available: 84.7GB
Nullsoft Install System v2.26
< Back
Install
Cancel
< Back
Finish
Cancel

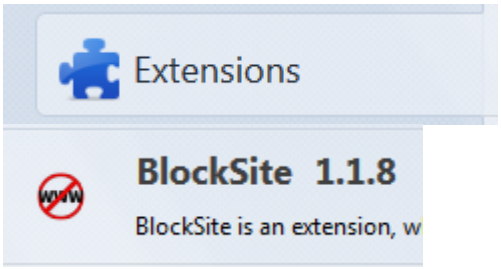

Fortress Secure Client 4.1
Copy
Create shortcut
Delete
Rename
keycall
Move to Startup

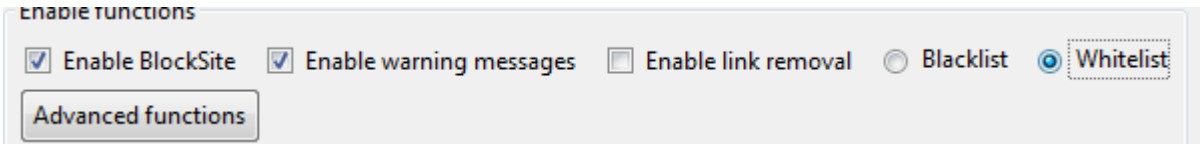

Last Name
Enter Last Name
Last F
Four SSN

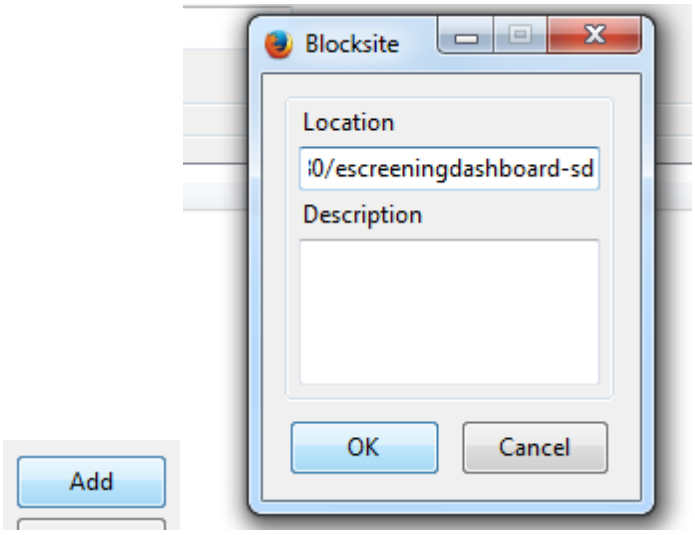
12) Installing Add-Ons for Firefox Interface



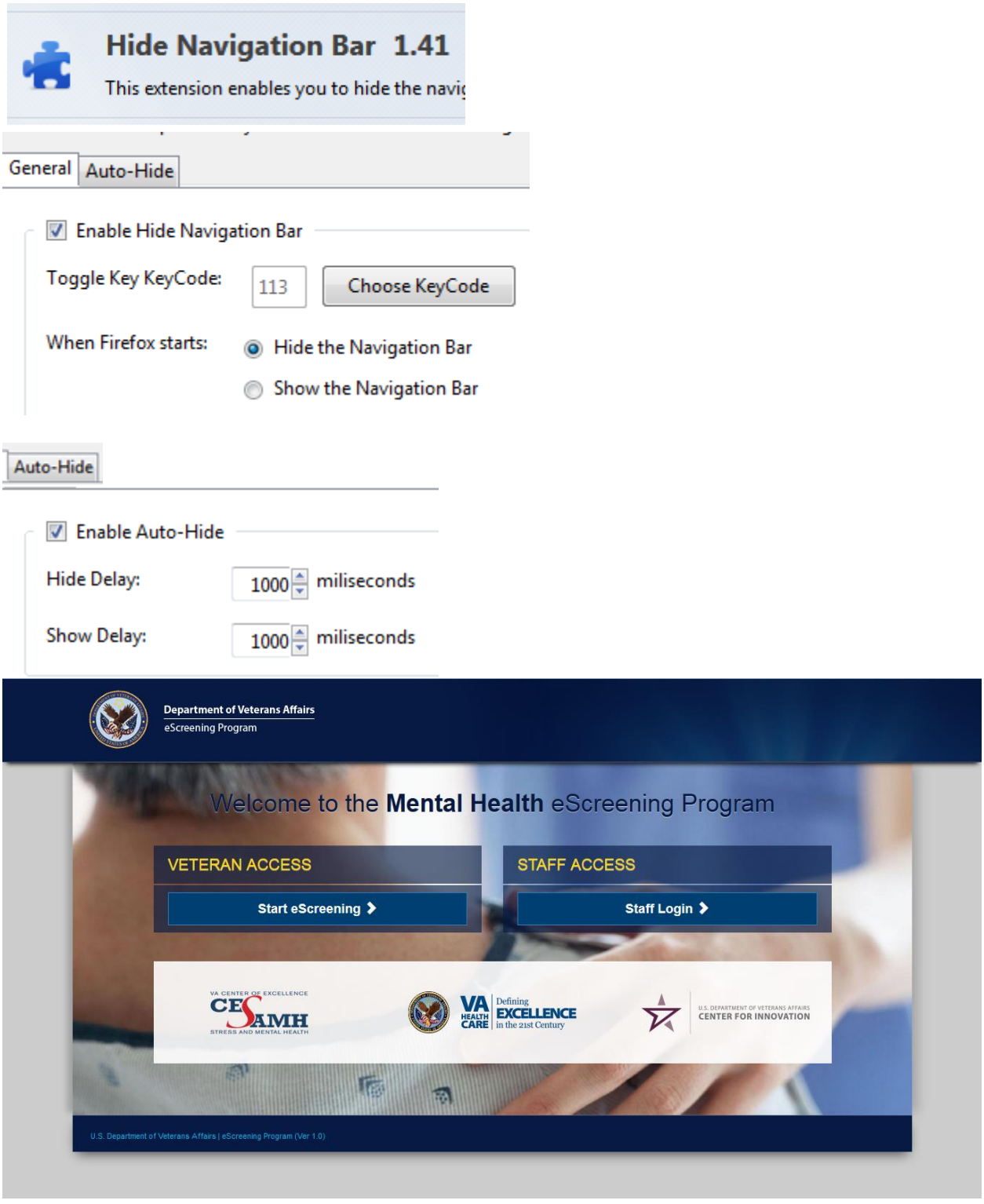
I don't want to help


Extensions
BlockSite 1.1.8
BlockSite is an extension, w

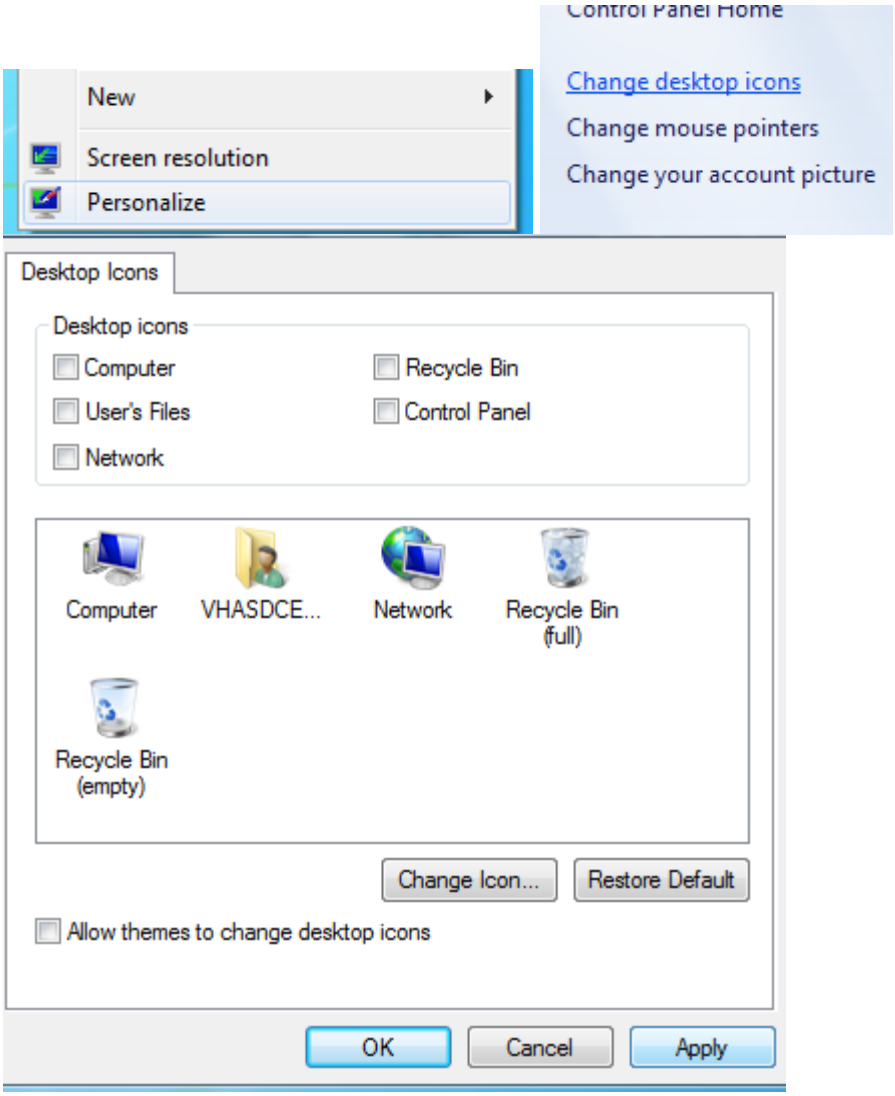

Enable functions
Enable BlockSite
Enable warning messages
Enable link removal
Blacklist
Whitelist
Advanced functions


Blocksite
Location
:0/escreeningdashboard-sd
Description
OK
Cancel
Add

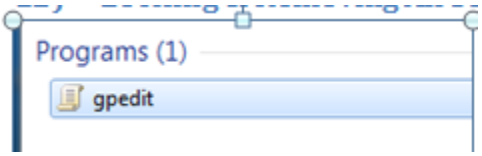
Hide Caption Titlebar Plus 2.8.6
"Maximize your screen space by controlling the presen
Hide Caption Titlebar Plus Options
Look & Feel
Look & Feel 2
Advanced Settings
Other Settings
Custom settings:
Show Custom Caption/TitleBar:
In Unmaximized windows
Small caption
Never
System borders:
Disabled
Activate custom borders and corner resizers
Make corners visible.
Border color
Disable Fx Window system-caption buttons (min,max,close), so customizable buttons can be used!
[1.1] Using a Glass-like window background (Recommended)
Custom Window background color
Active when no Persona-skin present. (default)
Custom Minimize, Max & Close Buttons: (located at top-right corner)
In Maximized window:
In Un-Maximized window:
Disabled
Disabled
Micro Close-button: floating buttons appears when hovering it or main menu is activated
• hovering activation delay-time (milliseconds)
0
• deactivation delay-time (milliseconds)
150
Skin:
New (Aero)
Define Action for Custom Close Button
Close Fx Window (Fx default)
Minimize Fx Window
Close Current Tab (recommended)
System TitleBar:
System TitleBar always hidden (Fx default: unchecked)
Firefox option: System TitleBar (almost) always present (recommended: unchecked)
Look & Feel
Look & Feel 2
Advanced Settings
Firefox
Options for Firefox 'Home Place' at top-left corner: (*)
Enable custom Firefox 'Home' Button.
Icon for Maximized win.
Icon for Un-Maximized win.
Firefox
Button Style/Color
Transparent with Personas skins
Floating Main Menu. Menu leaves Menubar and 'floats' alongside new 'Fx Home place' with autohide.
Activated by hovering over Fx Button (*), pressing ALT or F10 key.
• hovering activation delay-time (milliseconds)
0
• deactivation delay-time (milliseconds)
150
Web-Page-Title alongside Floating Menu
Full-Screen mode option:
Autohide also Firefox 'Home' Button and Custom-Min,Max,Close buttons when autohiding Toolbars in Full-Screen mode (default: yes)
Drag Fx window using Tab-bar background (default: no)
(& un/maximize it with double-click)

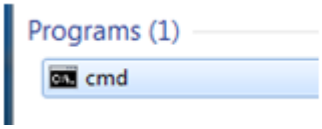

Hide Navigation Bar 1.41
This extension enables you to hide the navig
General
Auto-Hide
Enable Hide Navigation Bar
Toggle Key KeyCode:
113
Choose KeyCode
When Firefox starts:
Hide the Navigation Bar
Show the Navigation Bar
Auto-Hide
Enable Auto-Hide
Hide Delay:
1000
miliseconds
Show Delay:
1000
miliseconds
Department of Veterans Affairs
eScreening Program
Welcome to the Mental Health eScreening Program
VETERAN ACCESS
Start eScreening
STAFF ACCESS
Staff Login
VA CENTER OF EXCELLENCE
CESAMH
STRESS AND MENTAL HEALTH
VA HEALTH CARE
Defining EXCELLENCE in the 21st Century
U.S. DEPARTMENT OF VETERANS AFFAIRS
CENTER FOR INNOVATION
U.S. Department of Veterans Affairs | eScreening Program (Ver 1.0)

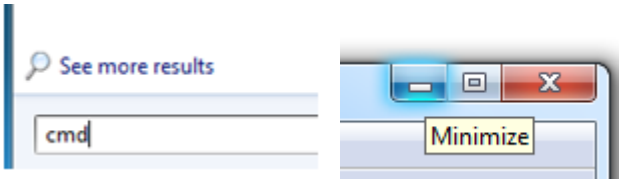
13) Removing Desktop Items

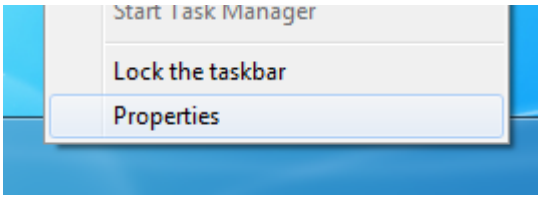


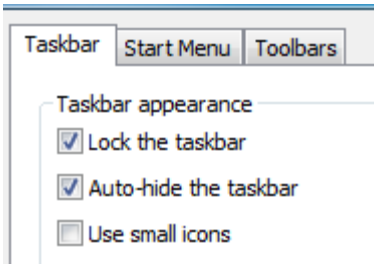
14) Locking & Removing All Settings

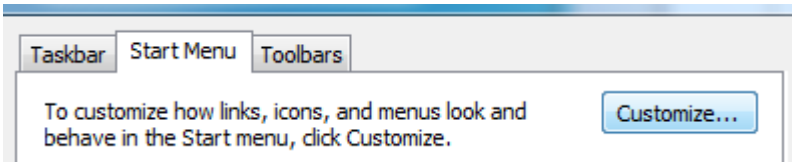


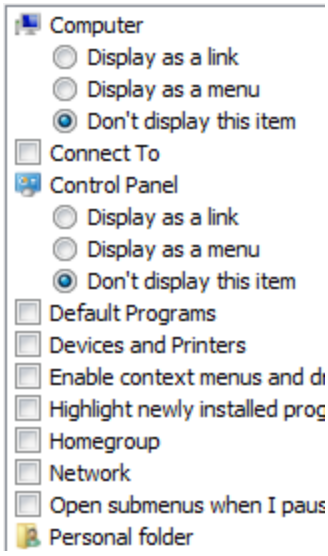


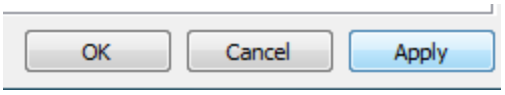


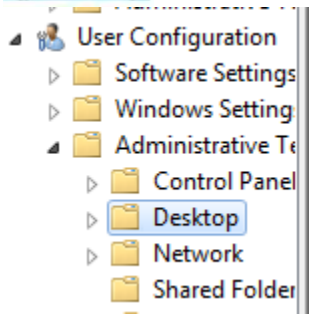


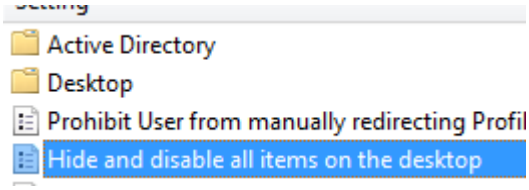


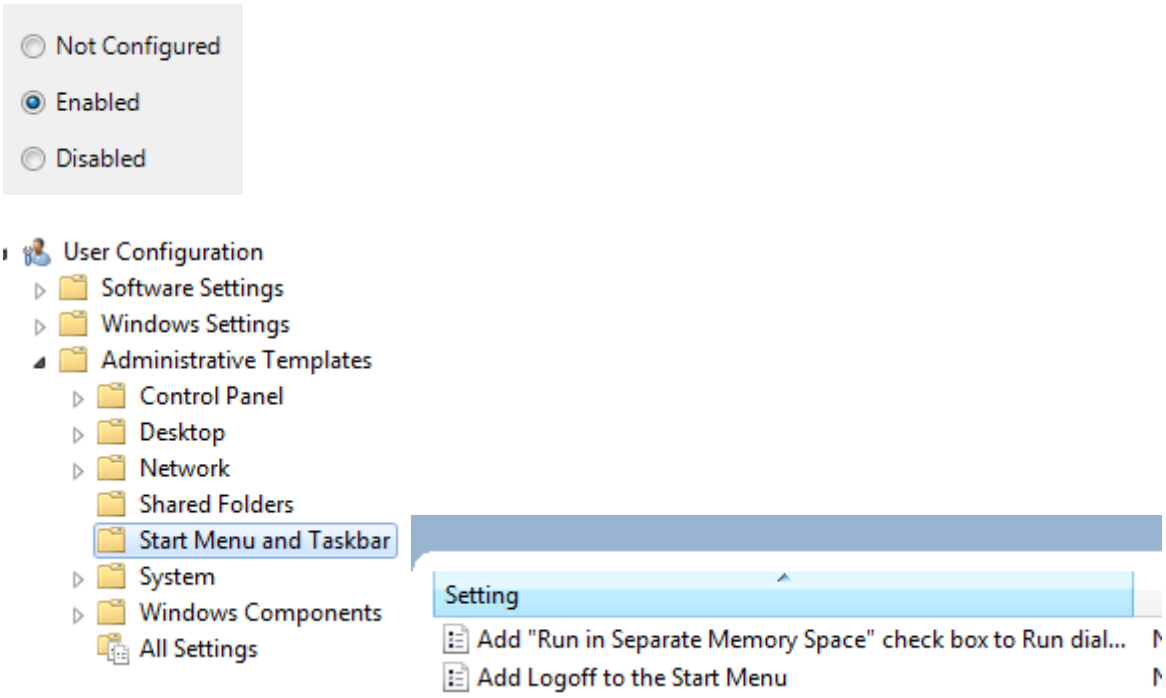

Taskbar
Start Menu
Toolbars
To customize how links, icons, and menus look and behave in the Start menu, click Customize.
Customize...

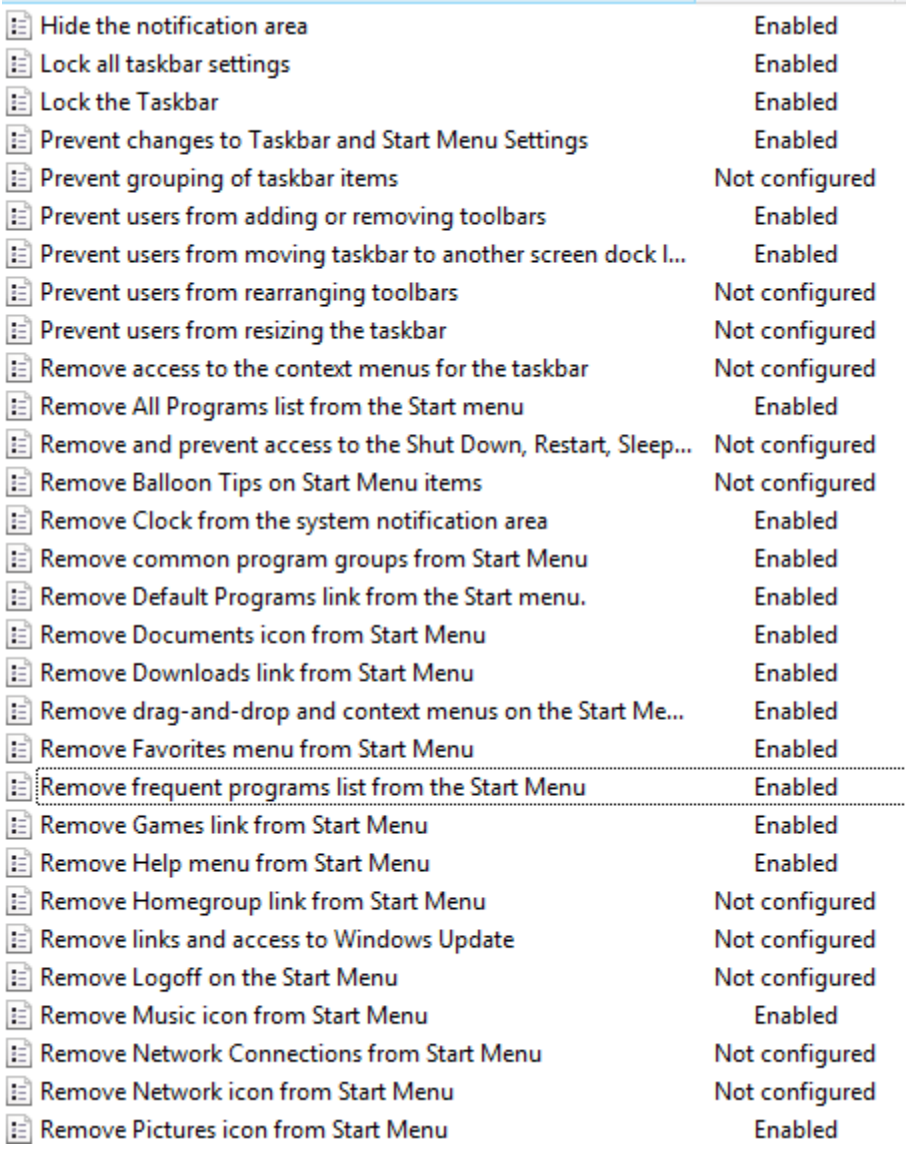

Computer
Display as a link
Display as a menu
Don't display this item
Connect To
Control Panel
Display as a link
Display as a menu
Don't display this item
Default Programs
Devices and Printers
Enable context menus and di
Highlight newly installed prog
Homegroup
Network
Open submenus when I paus
Personal folder


OK
Cancel
Apply


User Configuration
Software Settings
Windows Setting
Administrative Te
Control Panel
Desktop
Network
Shared Folder

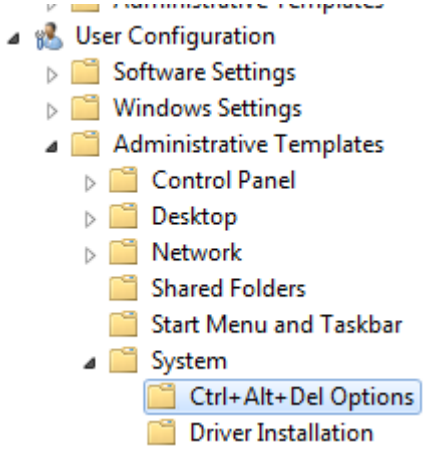

Active Directory
Desktop
Prohibit User from manually redirecting Profil
Hide and disable all items on the desktop

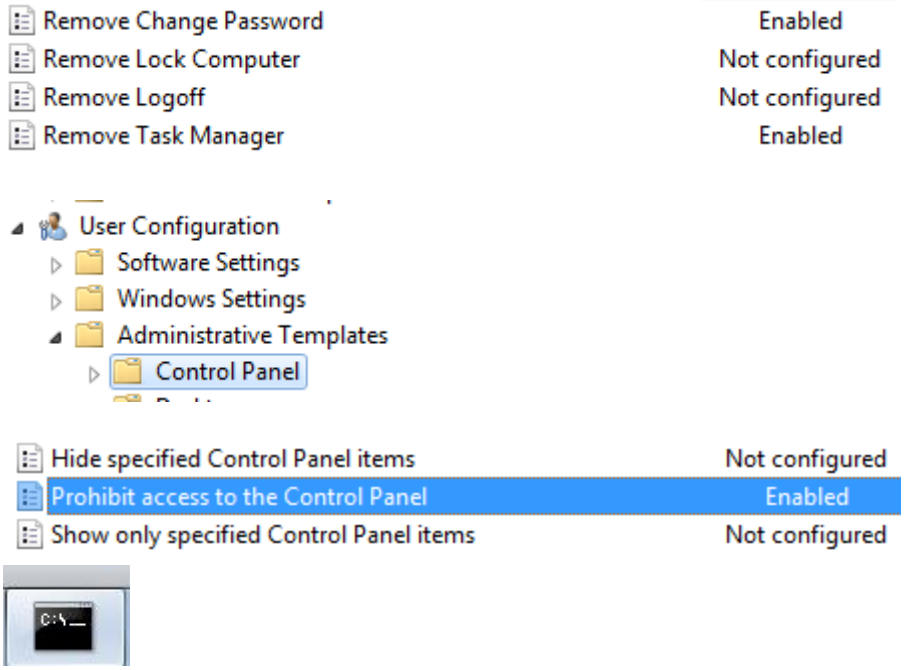

Not Configured
Enabled
Disabled
User Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Desktop
Network
Shared Folders
Start Menu and Taskbar
System
Windows Components
All Settings
Setting
Add "Run in Separate Memory Space" check box to Run dial...
Add Logoff to the Start Menu

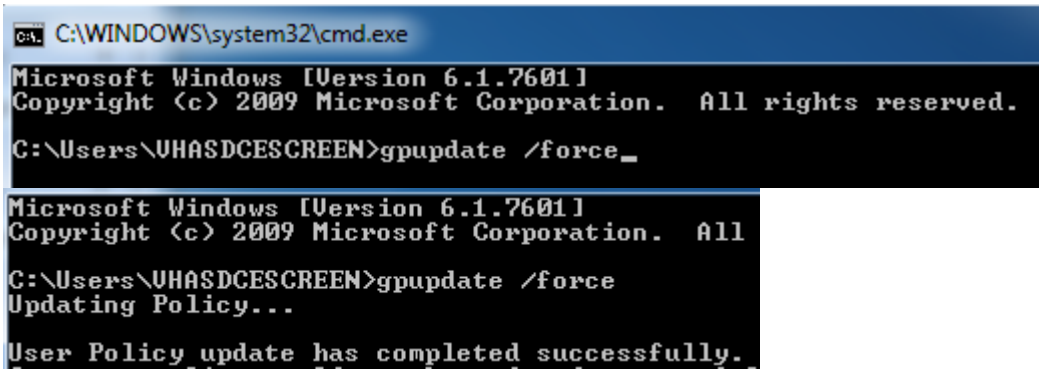


Hide the notification area	Enabled
Lock all taskbar settings	Enabled
Lock the Taskbar	Enabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Prevent grouping of taskbar items	Not configured
Prevent users from adding or removing toolbars	Enabled
Prevent users from moving taskbar to another screen dock l...	Enabled
Prevent users from rearranging toolbars	Not configured
Prevent users from resizing the taskbar	Not configured
Remove access to the context menus for the taskbar	Not configured
Remove All Programs list from the Start menu	Enabled
Remove and prevent access to the Shut Down, Restart, Sleep...	Not configured
Remove Balloon Tips on Start Menu items	Not configured
Remove Clock from the system notification area	Enabled
Remove common program groups from Start Menu	Enabled
Remove Default Programs link from the Start menu.	Enabled
Remove Documents icon from Start Menu	Enabled
Remove Downloads link from Start Menu	Enabled
Remove drag-and-drop and context menus on the Start Me...	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove frequent programs list from the Start Menu	Enabled
Remove Games link from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove Homegroup link from Start Menu	Not configured
Remove links and access to Windows Update	Not configured
Remove Logoff on the Start Menu	Not configured
Remove Music icon from Start Menu	Enabled
Remove Network Connections from Start Menu	Not configured
Remove Network icon from Start Menu	Not configured
Remove Pictures icon from Start Menu	Enabled

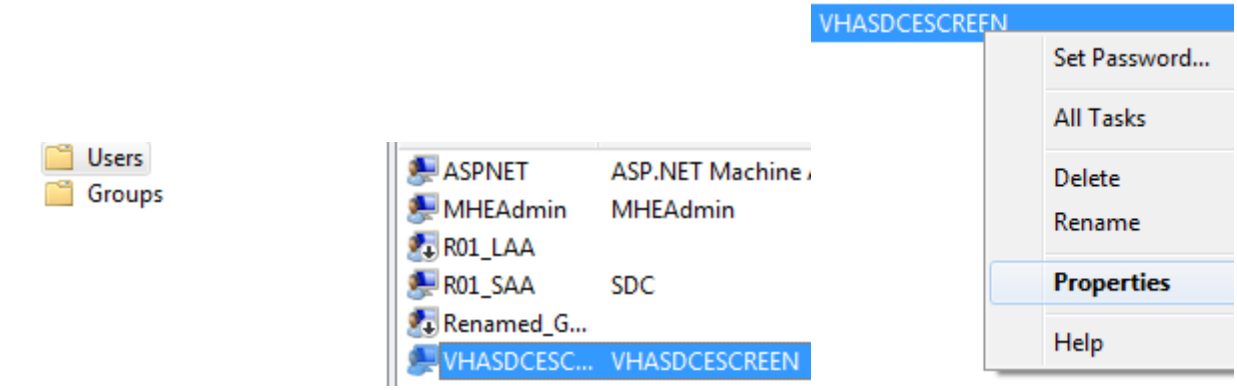
Remove pinned programs from the Taskbar	Not configured
Remove pinned programs list from the Start Menu	Not configured
Remove programs on Settings menu	Not configured
Remove Recent Items menu from Start Menu	Enabled
Remove Recorded TV link from Start Menu	Not configured
Remove Run menu from Start Menu	Not configured
Remove Search Computer link	Not configured
Remove Search link from Start Menu	Not configured
Remove See More Results / Search Everywhere link	Not configured
Remove the "Undock PC" button from the Start Menu	Not configured
Remove the Action Center icon	Not configured
Remove the battery meter	Not configured
Remove the networking icon	Not configured
Remove the volume control icon	Not configured
Remove user folder link from Start Menu	Enabled
Remove user name from Start Menu	Enabled
Remove user's folders from the Start Menu	Enabled
Remove Videos link from Start Menu	Not configured
Show QuickLaunch on Taskbar	Not configured
Turn off all balloon notifications	Enabled
Turn off automatic promotion of notification icons to the ta...	Not configured
Turn off feature advertisement balloon notifications	Not configured
Turn off notification area cleanup	Not configured
Turn off personalized menus	Not configured
Turn off taskbar thumbnails	Not configured
Turn off user tracking	Not configured

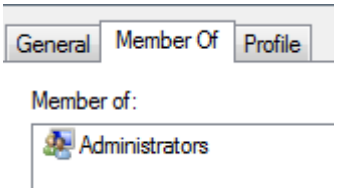


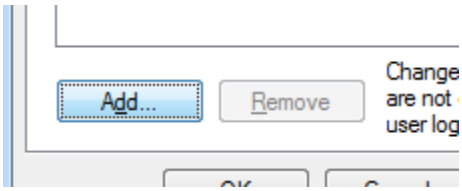


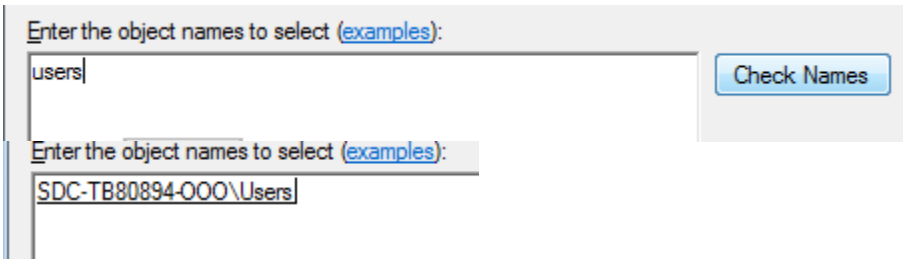


15) Revoking VHASDCESCREEN Administrator's rights

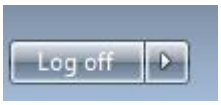

VHASDCESCREEN
Set Password...
All Tasks
Delete
Rename
Properties
Help
Users
Groups
ASPNET
ASP.NET Machine
MHEAdmin
MHEAdmin
R01_LAA
R01_SAA
SDC
Renamed_G...
VHASDCESC...
VHASDCESCREEN

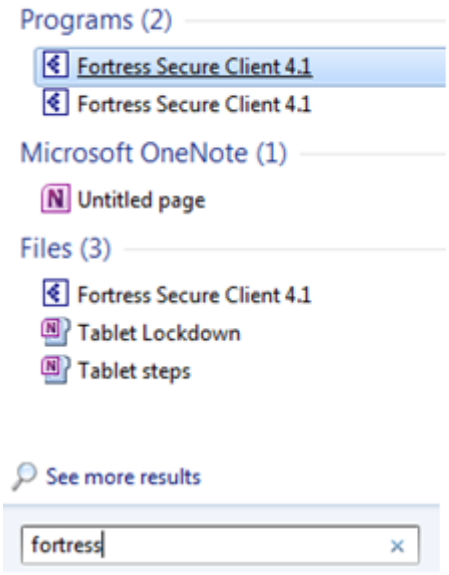

General
Member Of
Profile
Member of:
Administrators

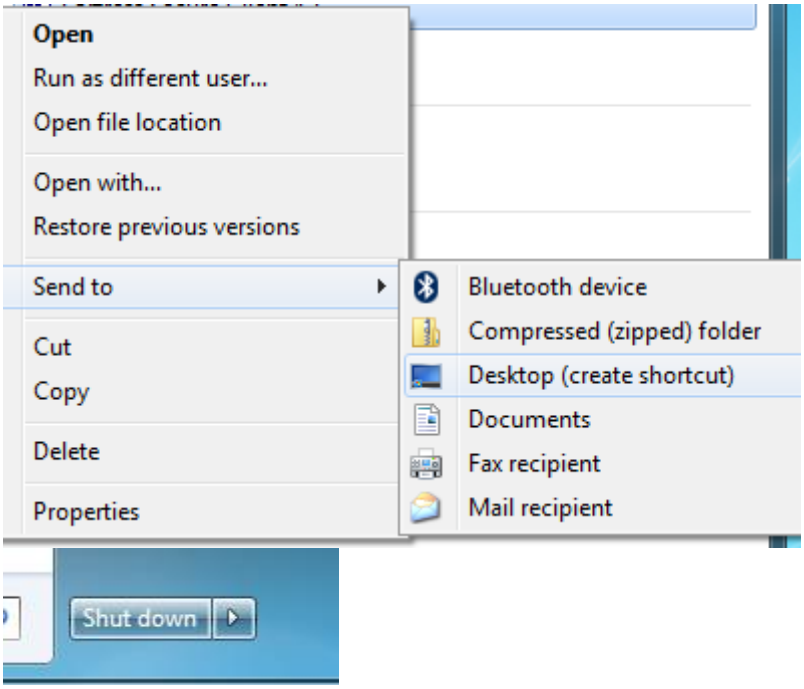

Add...
Remove
Change
are not
user log


Enter the object names to select (examples):
users
Check Names
Enter the object names to select (examples):
SDC-TB80894-OOO\Users

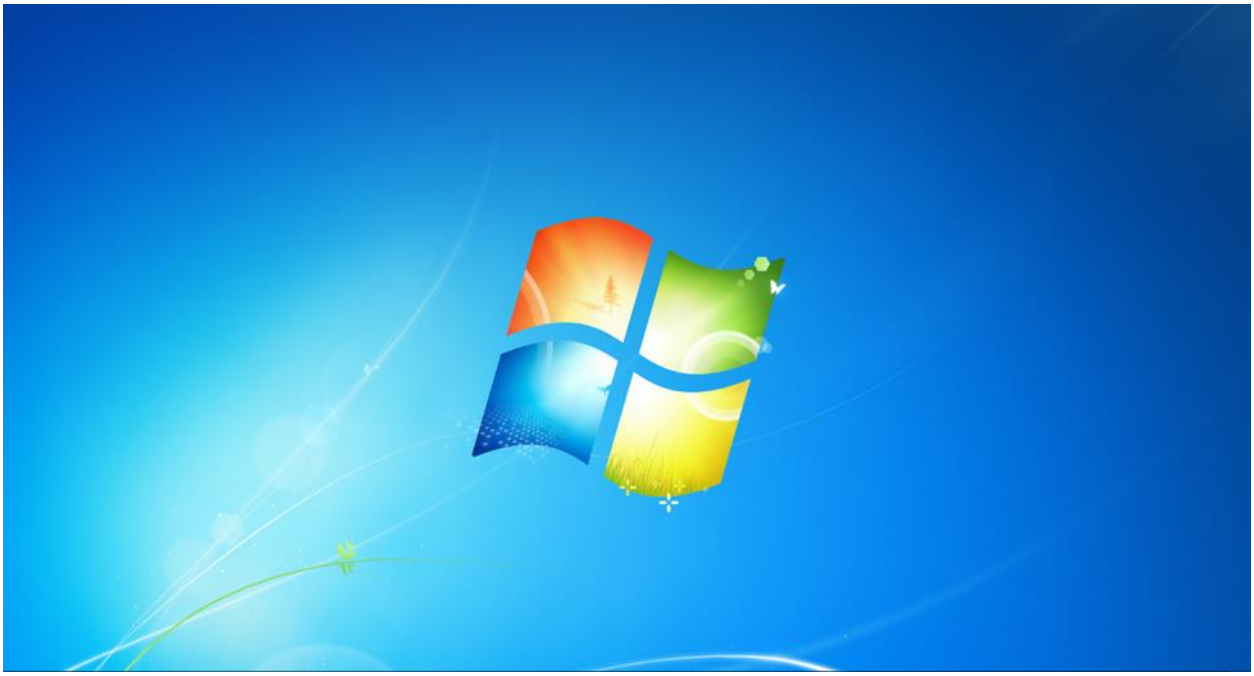
16) Perform the final lockdown step.




Programs (2)
Fortress Secure Client 4.1
Fortress Secure Client 4.1
Microsoft OneNote (1)
Untitled page
Files (3)
Fortress Secure Client 4.1
Tablet Lockdown
Tablet steps
See more results
fortress


Open
Run as different user...
Open file location
Open with...
Restore previous versions
Send to
Cut
Copy
Delete
Properties
Bluetooth device
Compressed (zipped) folder
Desktop (create shortcut)
Documents
Fax recipient
Mail recipient
Shut down

17) Test Locked Down Tablet



Samsung Tablets
Maintenance & Troubleshooting
Step-by-Step Guide

Note: Most Fixes Require Administrator's Rights, unless you know how to "Run as Administrator".

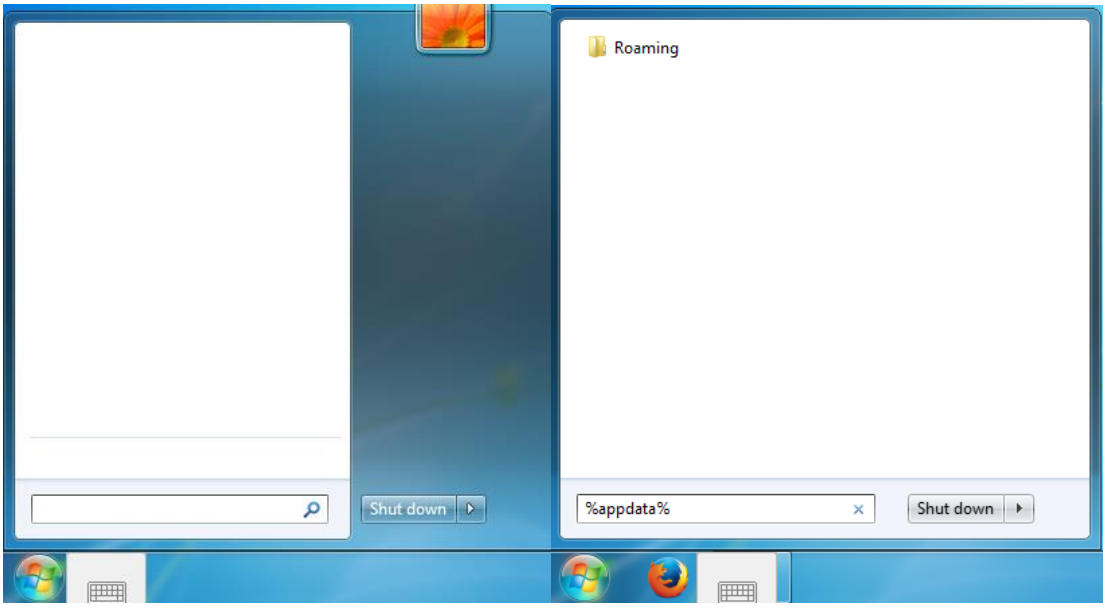
Reauthorize VHASDCESCREEN to Have Administrator's Rights

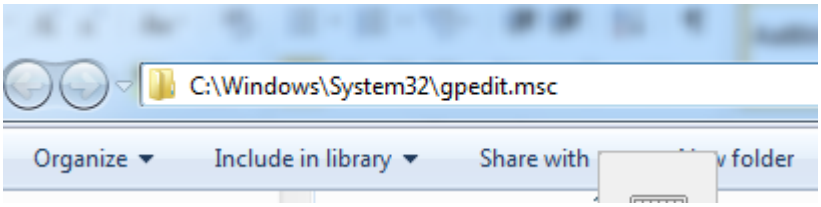
a) Log in as **Mheadmin**
b) Open Control Panel. Under Users, select **Change account type**. Then select **VHASDCESCREEN**, then click **Properties**
c) Under Group Membership, select **Administrator**
d) Click **OK** and log off, then log in as **VHASDCESCREEN**

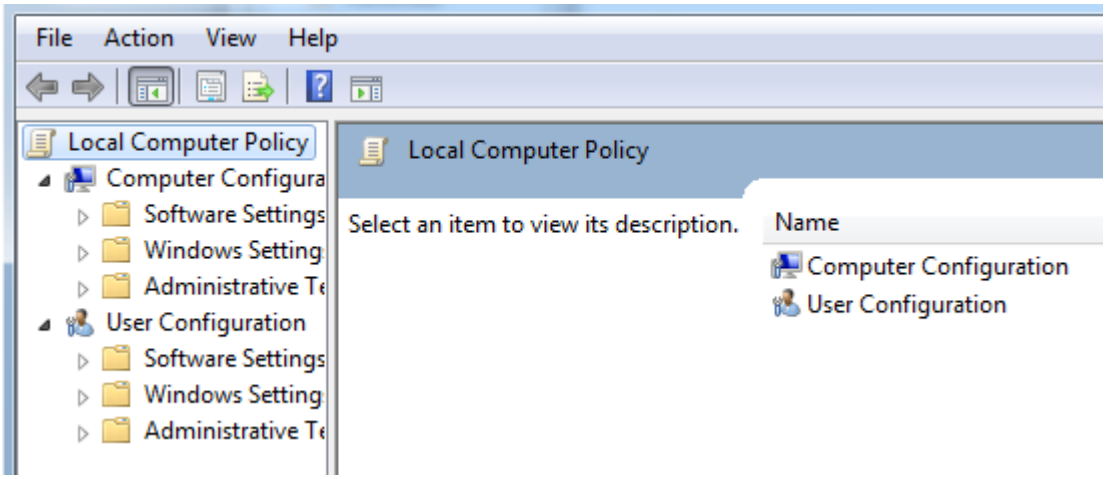
Backdoor to gpedit When Search Disabled

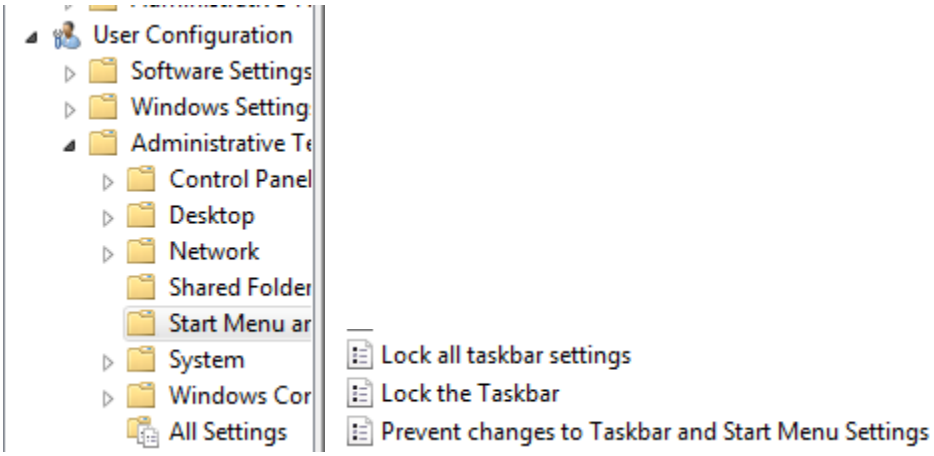
a) **Start**, type: **%appdata%** in the search box → **Enter**
b) Click in the browser bar and type: **C:\Windows\System32\gpedit.msc → Enter**
c) Disable any option required. Recommended:
    i) User Configuration > Administrative Templates > Start Menu and Taskbar (click the top "**Setting**" bar to alphabetize the options)
        (1) **Lock all taskbar settings**
        (2) **Lock the taskbar**
        (3) **Prevent changes to taskbar and start menu settings**
d) Log off and Log back in

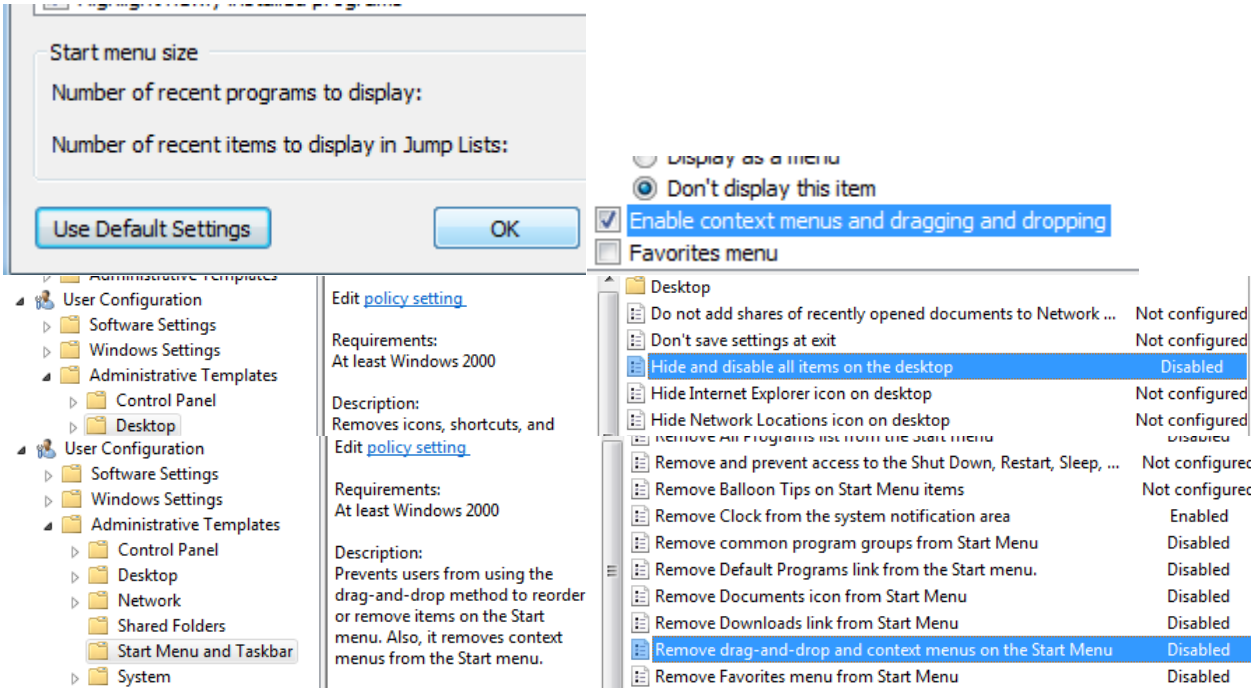
i) Right-click the **Taskbar → Properties → Start Menu Tab → Customize → Use Default Settings →** Check **Enable context menus and dragging and dropping → OK**











Startup folder not showing up in All Programs list

a) **Start → Search → gpedit.msc**

b) User Configuration > Administrative Templates > Start Menu and Taskbar (click the top "**Setting**" bar to alphabetize the options)

   i) **Disable**

      (1) **Remove user folder link from Start Menu**

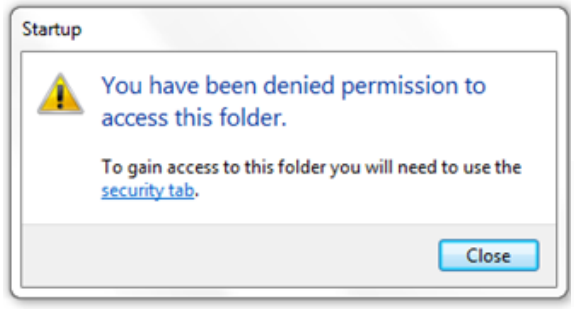
      (2) **Remove user's folders from the Start Menu**

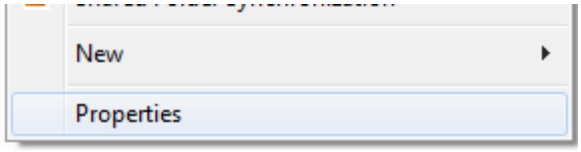
Remove user folder link from Start Menu	Disabled
Remove user name from Start Menu	Enabled
Remove user's folders from the Start Menu	Disabled

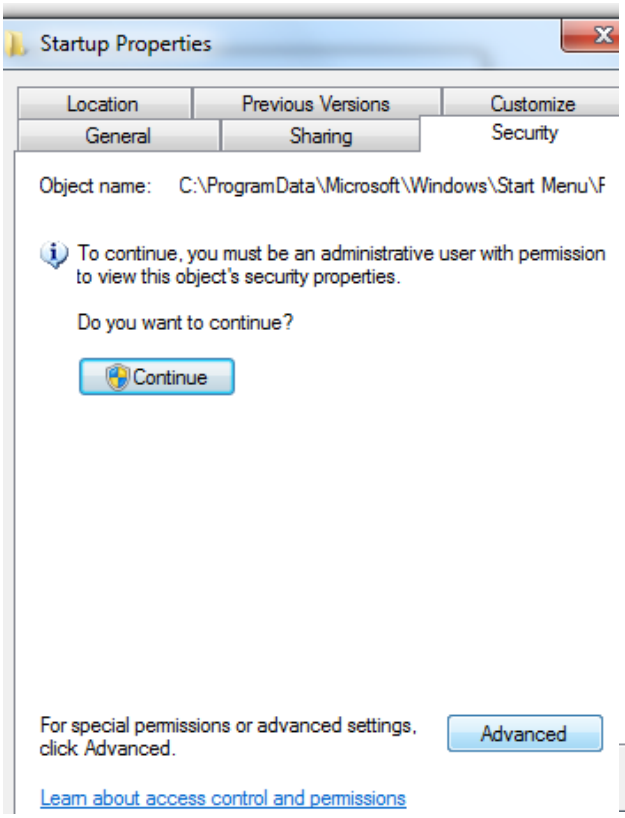
Cannot Add Shortcut in Startup Folder

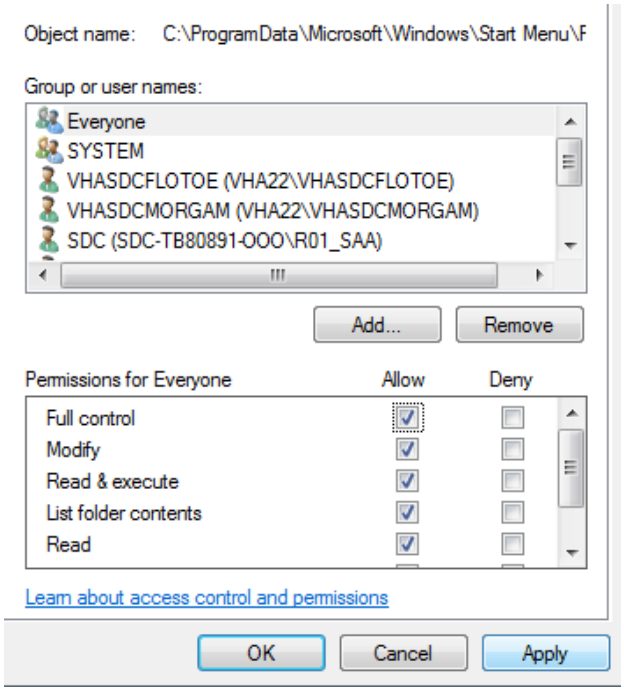
a) **Right-click** in the folder →**Properties** → **Security tab** → Find **VHASDESCREEN** click **Edit**

b) Click **Full control** under the **Allow** column → **Apply** → **OK**









Right-Clicking Does Not Do Anything (No Context Menus Available)

a) Right-click the **Taskbar → Properties → Start Menu Tab → Customize →** Check **Enable context menus and dragging and dropping → OK**

c) **Start → Search → gpedit.msc**

i) User Configuration > Administrative Templates > Desktop

(1) **Disable: Hide and disable all items on the desktop**

ii) User Configuration > Administrative Templates > Start Menu and Taskbar (click the top "**Setting**" bar to alphabetize the options)

(1) **Disable: Remove drag-and-drop and context menu on the Start Menu**

Keycall Error Message upon Installation

a) Abort the installation do one of the following:

i) Search for the keycall folder (if it is in any other folder than **My Documents**, cut and paste to the appropriate folder)

In the **System Tray** (bottom right corner), click the triangle → Right-click on the keycall icon → **Exit →** Redo step **D.** (**If this does not work, do step i**)

Attachment - Approval Signatures

Signature verifies acceptance of Implementation Plan:

_____	_____
Niloo Afari, PhD, Division Director, MHE Sponsor	Date
_____	_____
Clinton Latimer, VA MHE PM / COR	Date