Quick Start Guide
Thin-client
Traffic Situation Display
(TSD-U/F/C)

Project Identification:

Version 1.1

July 23, 2012

Prepared by:

CSC

Version	Date	Description of Change
1.0	6/29/12	Initial Version for TSD-U/F/C Deployment
1.1	7/23/12	Weather functions allowed

Application Version to create document:

Microsoft Word 2007

Table of Contents

1. Overview

This document describes how to connect to the thin-client Traffic Situation Display (TSD) which replaces the Web Situation Display (WSD) and Common Constraint Situation Display (CCSD). There are three general user categories referred to as TSD-U for unfiltered, TSD-F for filtered (no sensitive flights), and TSD-C for CDM (Collaborative Decision Making). Please refer to the TSD-U/F or TSD-C Reference Manual for detailed information on user functions.

A single TSD in a web browser is provided for each individual login into the system. Limitations are placed on functionality by “graying out” prohibited menu items.

2. Using Oracle Secure Global Desktop (SGD)

Thin-client TSD uses Oracle Secure Global Desktop (SGD) to provide secure, remote access to TSD functions. To access thin-client TSD, you need an account and a compatible browser with Java™ technology enabled.

This section guides you through the basics of using SGD. It describes how to log in and log out of the software, as well as how you can use SGD to run the TSD application.

2.1. Obtaining Access

Contact the TFM Consolidated Service Desk (TCSD), (609) 485-9601, to request a new account or modification to an existing user account. The TCSD will provide an application form for you to complete and submit through the appropriate management chain. Once approved, the TCSD will provide a user name, password and the URL through appropriate channels.

2.2. Requirements

Before you log in to SGD, ensure the following requirements are met:

- You have a compatible browser installed:

  Web Browsers – Firefox, Internet Explorer, Safari

SGD supports the following Operating System/Browser versions:

Microsoft Windows XP, Vista	Internet Explorer 7 & Internet Explorer 8, Mozilla Firefox 3
Microsoft Windows 7	Internet Explorer 8, Mozilla Firefox 3
Red Hat Linux 5.5 Desktop	Mozilla Firefox 3
Mac OS X 10.6	Safari 4 & 5, Mozilla Firefox 3

Note: other Browsers may work, but if a problem arises, there may be no support to correct the issue.

- JavaScript™ software is enabled in your browser; **Note:** If Java technology is not enabled in your browser, a warning message is shown. You must enable Java technology in your browser before proceeding. If JavaScript is not enabled in your browser, a warning message is displayed beneath the login dialog box.
- You have a user name and password for the SGD server. Contact your local administrator or the TCSD if you do not know your user name and password. Refer to Section 8 for the rules governing accounts and passwords.
- You know the Web Address for the login - the Uniform Resource Locator (URL) for the SGD server. Contact your local administrator or the TCSD if you do not know the Web Address / URL.

3.RSA Authorization

You may be required to have an RSA account to access thin client (RSA stands for "Rivest, Shamir and Adleman", who created the public key algorithm). If this additional authorization is required, you will be prompted for your RSA User ID and passcode, prior to seeing the SGD login, as illustrated in Figure 1.

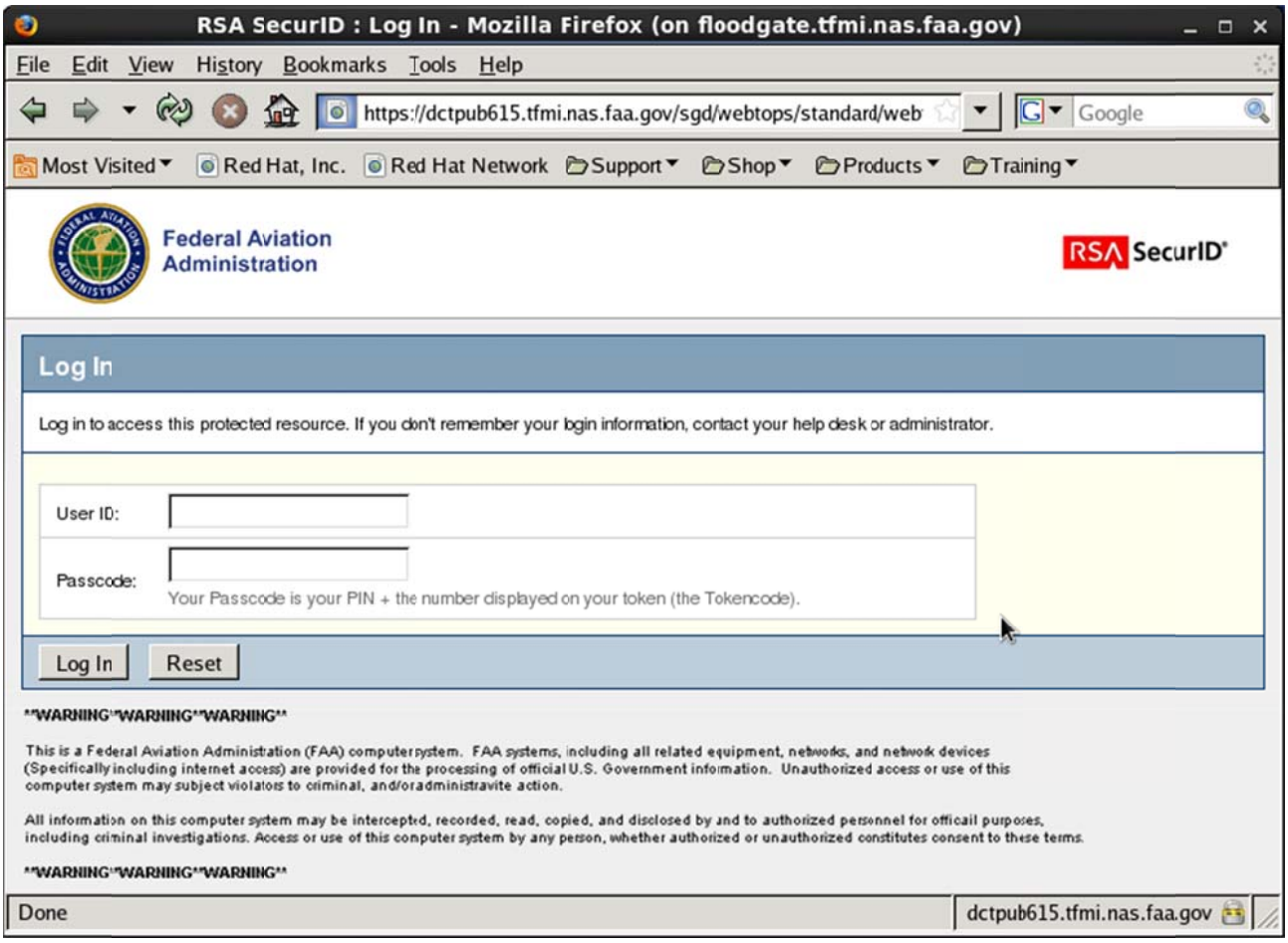

Figure 1. RSA Login

RSA Login screen.

1. Enter your assigned RSA User ID and SecureID token into the User ID and passcode fields, respectively.
2. Click the **Log In** button.
3. If verified, the system will proceed to the SGD Login.

4. SGD Login

To log in:

1. Using your browser, go to the SGD login URL. The Secure Global Desktop login menu will be displayed as shown below in Figure 2:

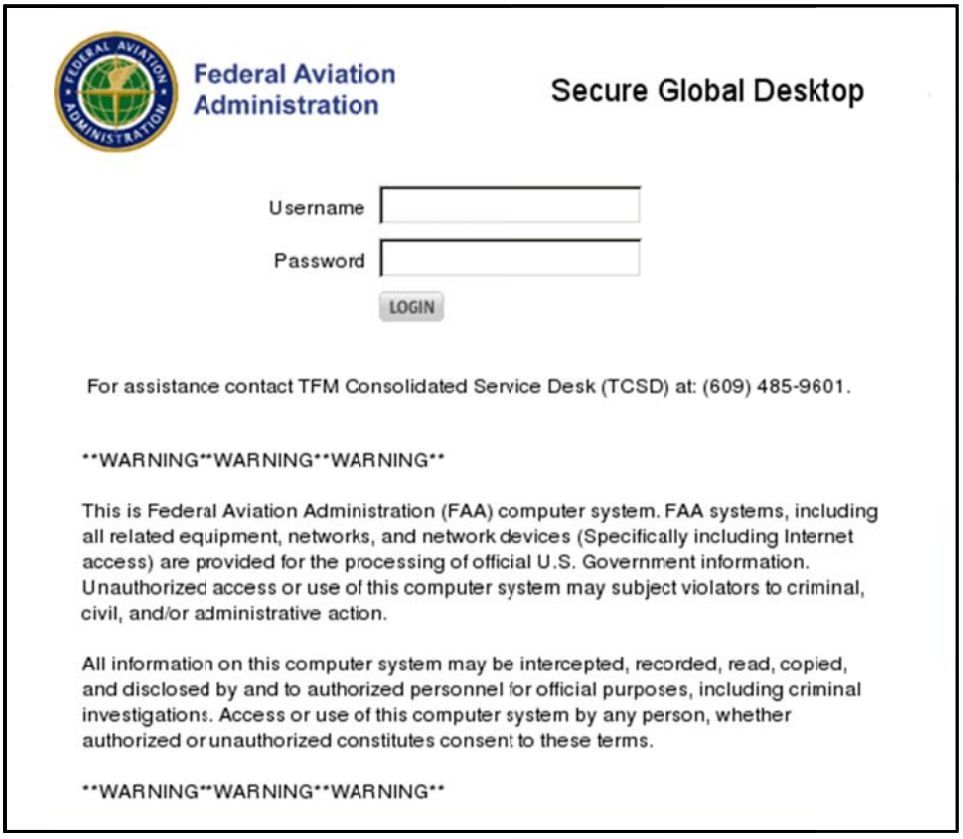

Figure 2. SGD Login Dialog Box

2. Type in your SGD Username and password.
3. Click the **Login** button
4. While SGD is starting up, the splash screen is shown (Figure 3)

Figure 3. SGD Splash Screen

The Initial Connection dialog box is shown (see Figure 4). This is a security message that is displayed the first time you connect to an SGD server.

Note: this may not open in front – check the Taskbar.

Figure 4. Initial Connection Dialog Box

1. Check **Accept this certificate permanently radio button**.
2. Click the **Accept** button.

Once you have accepted, you will not see the security message again unless there is a problem with the connection.

A Java technology security warning is shown (see Figure 5). This is a security message that is shown the first time you connect to an SGD server.

Figure 5. Java Technology Security Warning Dialog Box

Select the **Always trust content from this publisher** option and click Run. A Potentially Unsafe Connection message may be displayed (Figure 6).

Figure 6. Potentially Unsafe Connection Message

1. Click the **Accept** button to proceed.

4.The SGD Webtop

The webtop is a web page that lists the applications you can initiate through SGD. Figure 7 outlines the webtop.

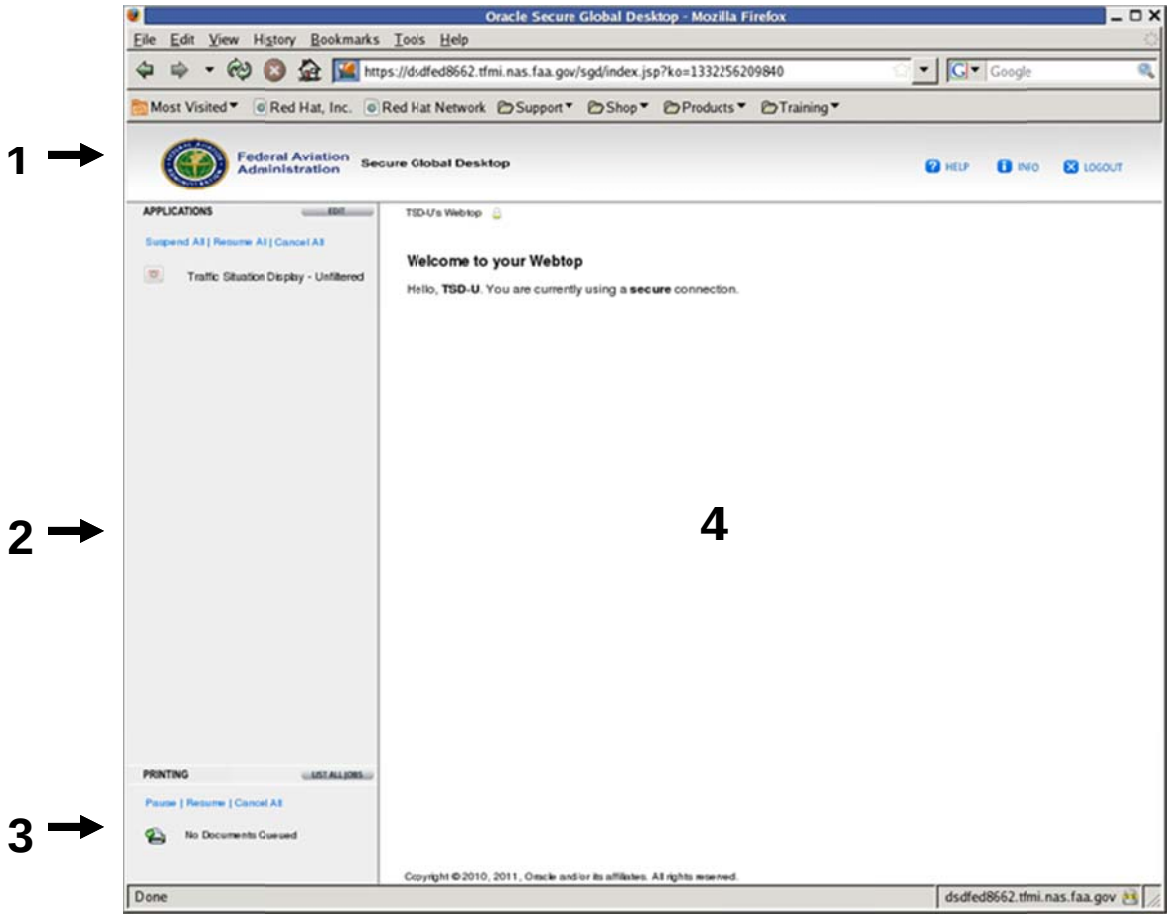

Figure 7. SGD Webtop

#	Name	Description
1	Menu bar	Includes Logout, Help, and Info buttons
2	Applications area	Lists the applications that you can run
3	Printing area	When you print from the TSD, your print file will be displayed in PDF format in an Adobe Reader. You can then either save the file or print to your local printer. The name of the print file will appear momentarily in the Printing area of the webtop.
4	Information area	Displays error messages and system information

5.Using Applications

Use the Applications area of the webtop to start, stop, and manage your applications.

5.1. Running Applications

To start an application, you click its link on your webtop, as shown in Figure 8. In a few moments the application is shown, ready for you to use.

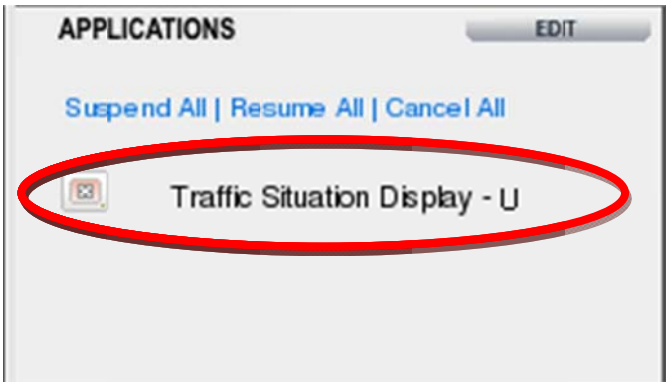

Figure 8. Application Area

5.2. Toolbars for Controlling Application

When an application is running, a triangle appears in front of the application's name on the webtop. A session toolbar also appears below the application name as shown in Figure 9.

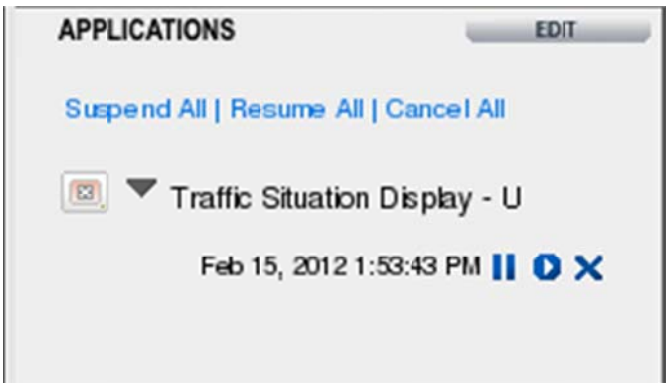

Figure 9. Toolbar session

5.3. Session Toolbars for Controlling an Application

The session toolbar allows you to:

- Click  to suspend an application
- Click  to resume an application
- Click  to end an application

5.4. To Log Out of SGD

Before you log out of SGD, ensure that you:

- Exit out of the application (Click “X” as illustrated for the Traffic Situation Display application in Figure 9 or close the TSD by hitting the X on the top right of the TSD window).
- Click the Logout button (Figure 10) on your webtop and click OK when prompted for confirmation
- Always log out of SGD before closing your browser

Figure 10. Logout Button

6. Thin Client Limitations

Former WSD and CCSD users will have no loss in functionality.

The thin-client does **not** have the following full-client TSD functions enabled:

- Replay (a.k.a playback)
- CIWS
- Reroute Preview, Model and attaching flight list
- Preference Sets
- Traffic Management Shell, TFMS Autosend, TFMS Electronic Mail and Route Manager
- Tools including Network Utilities, Database Commands, Script, EDCT Commands, with the following exception: TSD-U/F users do have access to the following EDCT Commands: EDCT CHECK, EDCT LIST, EDCT SLIST, EDCT SUB SHOW, and EDCT UNASSIGNED SLOTS.
- NAS Monitor, with the following exceptions: TSD-U and TSD-F users can use Time in Sector, Bar Charts, and Show/Hide Flights
- TSD-C users do not have access to the NAS Monitor
- TSD-U and TSD-F users have access to all NAS Monitor functions except for Turn Green
- Alarms functions
- Edit/Cancel/Delete Reroute
- Approve or revoke an exception, or Generate an Amendment from Reroute Monitor

Also:

- The only Semicolon Command allowed is Request List.
- TSD-C users do not have access to FLIGHTS menu functions
- TSD-C users cannot use Show/Hide Flights within Reroute Monitor or FEA/FCA Timeline

7. Login Security Policy

The following security policy is applied to all users:

1. Every user must be named and assigned a unique strong password: Minimum 10 characters, 1 uppercase, 1 lowercase, 1 number, and 1 special character (e.g., !, @, #, %, etc).
2. Accounts are locked for 30 minutes after 3 unsuccessful logins during a 2 minute period.
3. Your login session will be locked out after 15 minutes of inactivity.
4. Initial passwords will be assigned by the Help Desk and must be changed at the first login.
5. Password must be changed every 90 days. Passwords may be re-used after 10 password changes.
6. Accounts will be locked if no activity is detected for 90 days. After review, the account will either be closed or the user will be requested to re-submit an account request.
7. Contact the Help Desk for any login/password issues.