



Install (Site Only)

Getting Help

- Access the e-ISuite website at: <http://famit.nwcg.gov/applications/eISuite>
- Contact the Helpdesk at: (866) 224-7677

Before Beginning

Site only needs to be installed on the Site server. There is no need to install it on every computer at the site. All other computers will access Site by entering the appropriate server URL into an Internet browser (provided by the site administrator or ITSS) or double clicking the Site icon that is installed on the computer's desktop. You may also want to save the e-ISuite webpage to your browser favorites.

e-ISuite System Requirements

To install and run Site, the PC must have the following minimum system requirements:

- Internet Browser – **Chrome is the only supported browser**
- Administrator privileges
- Java Script enabled in the browser

Key Points to Remember for ITSS

- Backup the incident database many times during the day, especially after significant data entry (preferably hourly).
- Setup Auto backups to an external location (i.e., USB drive, external hard drive) as often as necessary or frequently save manually backed up files to an external location.
- Backup MANUALLY before performing any administration action.

Downloading Site

To Download the Site Application from the e-ISuite Website

1. Start an Internet browser.
2. In the Address box, enter <http://famit.nwcg.gov/applications/eISuite>.
3. On the Welcome to e-ISuite webpage, click the link for the Site Download.
4. Download the e-ISuite Site installer.
5. Save the File to the desktop.

Installing Site

To Install the Site Application

1. To run the Site installation, users will need to follow agency specific processes for software installations.
2. Follow the Install wizard to install the Site application on the user's machine.
3. Click the **Finish** button when the message displays.

Logging into Site

If this is the first time logging in after installing Site, create an Account Manager User. This will require the creation of an initial database name, password, and the initial Site Account Manager user. It may also be necessary to turn off pop-up blockers for the e-ISuite application.

Logging into Site cont'd

1. Launch Site.
2. Enter the **Database Name**, **Database Password** and **Confirm Database Password** to create the initial database.
3. In the User Name field, the system will default a prefix of '.ad' to identify the account as a privileged account. Do not remove the '.ad'. Complete this field by entering the remainder of the **User Name** after the prefix (e.g.
4. ad.username). Enter the **First Name**, **Last Name**, **Unit ID**, **Password** and **Confirm Password**.
5. Click **Save**.



Create Account Manager User

Please create the initial database name, password, and the initial Site Account Manager user.

Database Name *

Database Password *

Confirm Database Password *



User Name *

First Name *

Last Name *

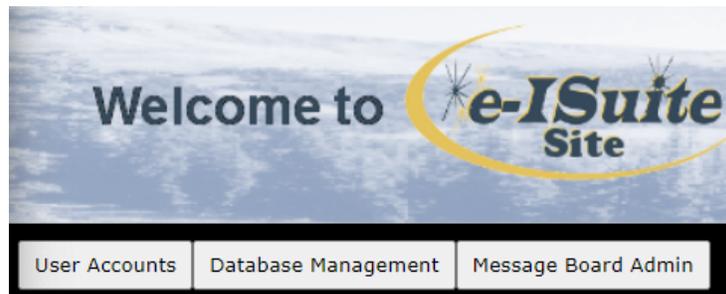
Unit ID *

Password *

Confirm Password *

Account Manager Homepage

1. Launch Site.
2. Select the **Database** from the drop down list.
3. Enter the **User Name**.
4. Enter the **Password**.
5. Click **Login**.



User Accounts/Database Management

User Accounts

On the Site homepage click the **User Accounts** button to access functions related to User Accounts. These functions include the ability to **Add**, **Edit** and **Delete** a user, **Export/Import User Accounts**, manage **User Sessions** and perform **User Auditing**. See the Account Manager - Site User Guide or Quick Reference Card for additional information on creating user accounts in Site.

Database Management

The **Database Management** button allows the user the ability to perform functions related to the database. These functions include **Create New DB**, **Copy DB**, **Edit DB**, perform a **Manual Backup**, **Restore DB**, **Remove DB**, **Recover DB Password** and **Merge Databases**. See the Account Manager - Site User Guide or Quick Reference Card for additional information on database management.

A user account with the Data Steward role needs to be created to manage incident data.