Software Installation Guide

System Requirements

With the exception of PERMS Integrator, all the TwinEngines products are web based applications that require a Microsoft Windows 2000 or 2003 web server and a Microsoft SQL Server 7.0 or 2000 database server. This guide is only for the Web based applications. See the PERMS Integrator guide for more information on how to install it.

Prior to installing the TwinEngines software, perform the following:
1. Identify the web server that the system will run on.
    a. Windows 2003 NOTE: Be sure that the "Enable Network DTC access" option is turned on. To set this option, open Add Remove Programs, select Add Remove Windows Components, highlight Application Server and click Details. Be sure to "Allow" Active Server Pages in IIS. To set this option, open IIS Manager, select Web Service Extensions, select "Active Server Pages", and select "Allow", stop and restart IIS.
2. Ensure that the web server has a secure certificate installed on it so that the applications can use SSL. All the applications require an SSL layer (e.g. https:).
3. Identify the database server that the applications will use.
    a. Windows 2003 NOTE: Be sure that the "Enable Network DTC access" option is turned on. To set this option, open Add Remove Programs, select Add Remove Windows Components, highlight Application Server and click Details.
4. Obtain the sa password for the database server so that the installation programs can create the database objects required by the applications.
5. Create a SQL Server user called cmsuser. Be sure to keep the password for this user around – you will be prompted for it during each one of the product installations.
6. SQL Server authentication should allow SQL Server logins. To set this option, open Enterprise Manager, select the server under SQL Server Group, right click the server and bring up Properties, select the Security tab, under Authentication select "SQL Server and Windows", stop and restart the SQL Server.
7. Locate the SIDPERS extract files (e.g. hsdosf, hsdspff, etc.) that are created for the load of the AITS server. These files are created on the SIDPERS system by running the ups.sh shell scripts.
8. Obtain an FTP login that can be used to download the SIDPERS extract files on a daily basis.
9. Obtain a login to the AITS and SIDPERS database servers that the TwinEngines applications can use.
10. Install the Oracle client (8i or 9i) on the database server. You must load the appropriate registry files base off of your Oracle client. These files are supplied in the Program Files\CMSWebServices folder. If you installed the Oracle 8.0 client, use the Oracle_8_0.reg. If you installed the Oracle 8.1 client use Oracle_8_1.reg, and for Oracle 9, use Oracle_9.reg. Stop and restart SQL Server after installing these registry keys.
11. Configure 2 SQL*Net aliases on the database server:
    a. SIDPERS – your SIDPERS system
    b. RCASDBOR – the AITS database server
12. Create a network service account that the TwinEngines applications will run under. You will need the network account login and password during the installation of CMSWebServices.
13. Add the network service account to the local "Power Users" group on the web server.

Downloading Installations

The installation programs can be downloaded from Downloads section at http://sharepoint.twinengines.com/NG. Download and extract the products you are going to install. Be sure to include the CMSWebServicesSetup and CMSWebServicesLoaderSetup as these programs are required to run any of the applications. You will also need the CMSInstall.zip. This is a database backup of a blank CMS database that you will restore to your database server.

Creating the SQL Databases

Before running the installations, create 2 databases – CMS and CMSWebServices. These databases are used by all products and are required. Next, create a database for each product you are going to install. The following table lists the product and the name of the database to create:
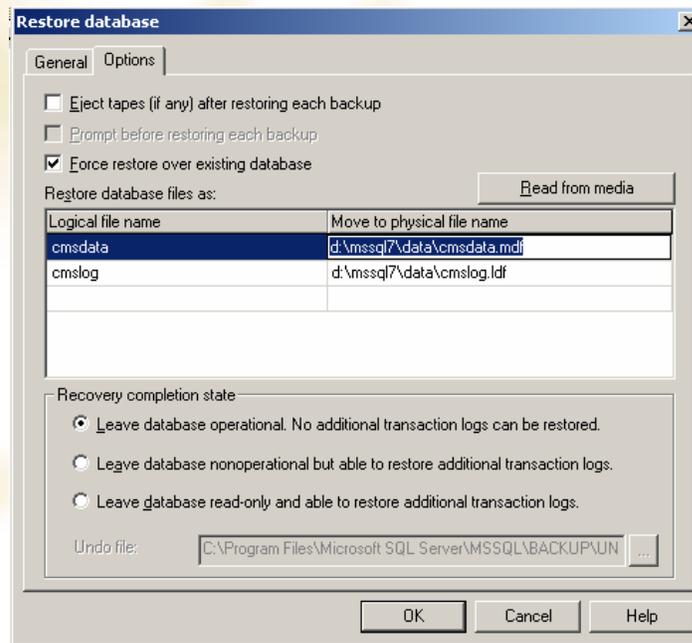
Application	Database Name
Awards Tracking	Awards
Discharges	Discharges
DA2-1	DA21
E-Trans Manager	ETransMgr
MILPO Admin	MILPOAdmin
NCOER	NCOER
OER	OER
Training & Security Tracking	TrainingTracking

If you are unfamiliar with how to create databases in SQL Server, see the online help under SQL Enterprise manager.

Once the databases are created, you will need to restore the CMS database from the backup found in the CMSInstall.zip file. Extract the CMSInstall.zip file onto a local drive of the SQL Server (you can't use the restore function with network drives). Use SQL Enterprise Manager to restore the database by right clicking on the CMS database and selecting "All Tasks -> Restore". You should see the following dialog:
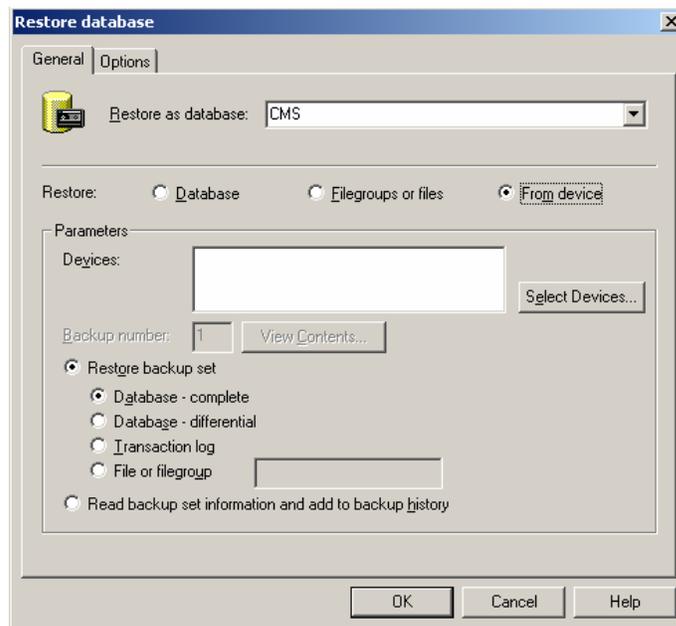
Check the "From Device" option and then hit "Select Devices". Browse to the file you extracted from the CMSInstall.zip. Select the "Options Tab" and you should see the following:

Restore database

General | Options

☐ Eject tapes (if any) after restoring each backup

☐ Prompt before restoring each backup

☑ Force restore over existing database

Restore database files as: Read from media

Logical file name	Move to physical file name
cmsdata	d:\mssql7\data\cmsdata.mdf
cmslog	d:\mssql7\data\cmslog.ldf

Recovery completion state

◉ Leave database operational. No additional transaction logs can be restored.

○ Leave database nonoperational but able to restore additional transaction logs.

○ Leave database read-only and able to restore additional transaction logs.

Undo file: C:\Program Files\Microsoft SQL Server\MSSQL\BACKUP\UN [...]

[OK]   [Cancel]   [Help]

Check the "Force restore over existing database", then change the path under the "Move to physical file name" to the correct path for the CMS data and log files. If you don't know the location of the data and log files for the CMS database, close this dialog and right click on the CMS database and select properties. The "General" tab will show you the location of the data file and the "Transaction Log" tab will show you the location of the log file.

Installing CMSWebServices

You are now ready to begin installing the TwinEngines products. The installation programs all run on the web server, not the database server. Start with the CMSWebServices installation. CMSWebServices contains shared components that all the other applications use. **When you upgrade your software, always be sure to upgrade CMSWebServices first**.

When the installation package begins, be sure to select your State/Territory from the User Information dialog. Your license key is tied to this information as well as some system defaults (e.g. the "State" in the Discharges application).

The first time you run the CMSWebServices installation, you will be prompted for the network service account that was created to run the TwinEngines software. You will see the following dialog:
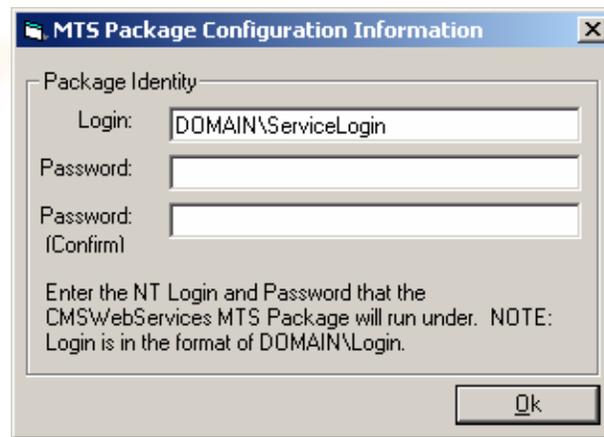
Enter in the domain name\service login (e.g. MYNGDOMAIN\MyServiceLogin) and the password and hit ok. If you get an error message that states something like "Method ~ of Object ~ failed", it most likely means that you entered the login or password incorrectly. Continue with the installation. Once the installation is complete, use the menu option of Start->Program Filies->CMSWebServices->Configure MTS Components to re-enter the information. If you can not connect to SQL Server you may have to install the SQL Server Client to the web server, contact your Administrator.

You will also be prompted for the login and password used by the CMSWebServices application. You will see the following dialog:
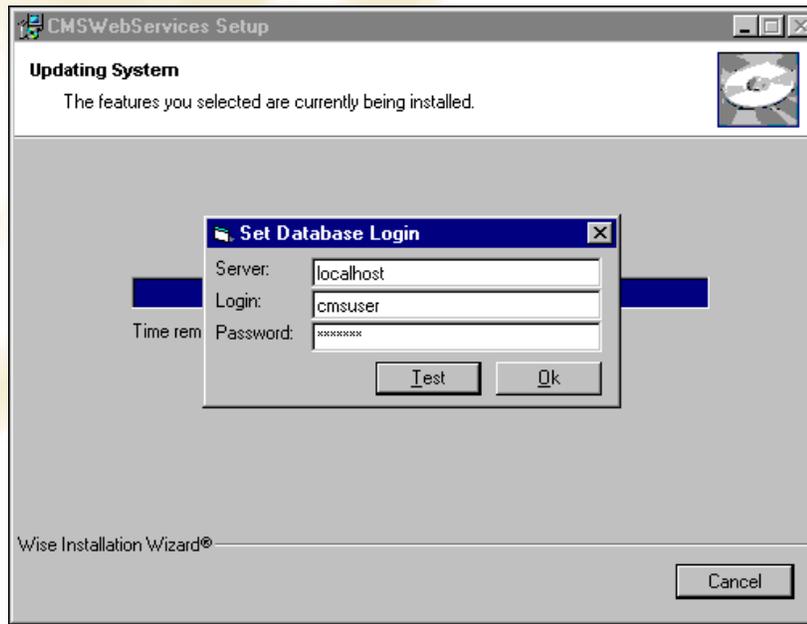
Enter the name of the database server and the cmsuser password that you created in SQL Server.

You will then be prompted for the SQL Administrator's login:

Enter the name of the database server and the password for the sa SQL Server login. The system will then run a series of database scripts that will create the database objects for you.

If you do not have the sa password at this time, you can hit Cancel and continue with the installation. When the installation is complete, you can use the menu option Start->Program Files->CMSWebServices->Install/Upgrade database to run the build database scripts.

During the installation, you will be prompted to create an Admin login. You will see the following dialog:

Enter your network login so that you can log into the User Administration and begin configuring additional users to use the application. You can access this feature after the installation with the menu option Start->Program Files->CMSWebServices->Create Admin User.

CMSWebServices Loader Installation

Before installing the products, you need to install the CMSWebServices Loader and import the data. Install the Loader on the web server. The installation is straight forward – you will not be prompted for anything but the installation path.

Once the installation has completed, you will need to compare the file names of the SIDPERS extract files to what is expected by the loader. The table in the CMS database, tblImportRef, holds the names of the files that the loader expects to load. During the installation of the AITS software, and depending on where you download the files from, these file names may need to be changed. By default, the loader does not expect an extension on the files.

Use SQL Enterprise manager to view the file names and change them if necessary. Open SQL Enterprise Manager and expand the tree until you see the tables under the CMS database. Find the table, tblImportRef, then right click on the table and select "Open Table->Return All Rows". You should see the following:

SQL Server Enterprise Manager - [Data in Table 'tblImportRef' in 'CMS' on '(local)']

File   Window   Help

| itrstrFile_Name	itrstrTable_Name	itrstrSpec_Name	itrintLength_Of_Lin	itrintRef_ID	itrstrKey_Name
awards	tblTempAwards	tblImportAwards	340	1	itaintSeq_No
exdate	tblExDate	tblImportExDate	12	2	iteintSeq_No
hsdasf	tblStrength	tblImportStrength	115	3	itsintSeq_No
hsdosf	tblOrganization	tblImportOrganization	161	4	itointSeq_No
hsdspff	tblSIDPERS	tblImportSIDPERS	827	5	itsidintSeq_No
lsdb	tblLSDB	tblImportLSDB	462	6	itlsdbintSeq_No
lsdb	tblTempFLAGS	tblImportFLAGS	462	7	itfintSeq_No
lsdb	tblTempImmunization	tblImportImmunization	462	8	itimintSeq_No
lsdb	tblTempLanguage	tblImportLanguage	462	9	itlaintSeq_No
attach	tblSIDPERS	tblImportSIDPERS	827	10	itsidintSeq_No
attaward	tblTempAwards	tblImportAwards	340	11	itaintSeq_No
attlsdb	tblLSDB	tblImportLSDB	462	12	itlsdbintSeq_No
attlsdb	tblTempFLAGS	tblImportFLAGS	462	13	itfintSeq_No
attlsdb	tblTempImmunization	tblImportImmunization	462	14	itimintSeq_No
attlsdb	tblTempLanguage	tblImportLanguage	462	15	itlaintSeq_No
hsdsplf	tblLossData	tblImportLossData	832	16	itldintSeq_No
hsdsplf	tblSIDPERSLoss	tblImportSIDPERS	827	17	itsidintSeq_No

Change the field named itrstrFile_Name to the correct file name for the files you are getting from SIDPERS.

You will now need to run the first import of data. See the Help files in the Loader for more information on how to configure the Loader and run the Import.

Product Installations

After the loader has completed its first load, you can now install the actual products. The product installations will prompt you for your license key during the setup, so be sure to have your license keys available. They will also prompt you for the database server name and cmsuser password, as well as the "sa" password for the SQL Server.

If the product accesses the SIDPERS or AITS databases, you may be prompted with the following dialog:
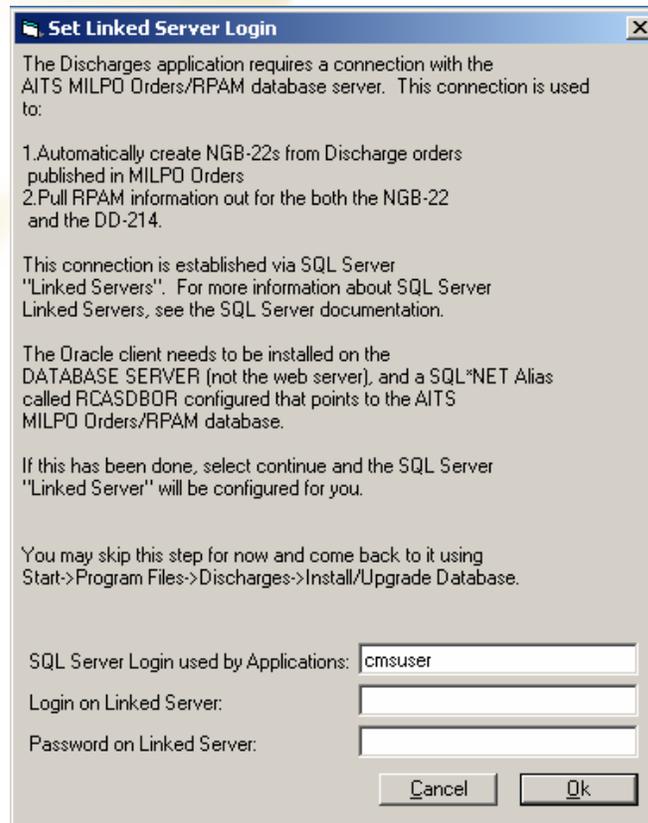
The TwinEngines Products use "Linked Servers" in SQL Server to access the SIDPERS and AITS databases through SQL Server. This allows the applications to query both the SQL Server database, the AITS database, and the SIDPERS database through a single interface.

SQL Server maps a SQL Server login (e.g. cmsuser) to an Oracle login (e.g. rcasadm). The applications use the cmsuser login when querying data from SQL Server. When a request is made by the application, SQL Server maps the cmsuser login to the appropriate Oracle login, logs into Oracle, executes the query, and returns the results as if you were querying a single SQL Server.

The above dialog will map the cmsuser login to a valid Oracle login. In order to create stored procedures that access the Oracle database, it will also map the "sa" login to the same Oracle login. The "sa" mapping is required because SQL Server will test the connection to Oracle when creating the stored procedure. If the "sa" mapping does not exist, you will get an error when the SQL script that creates the stored procedure is run.

You can view these mappings in SQL Enterprise Manager. Expand the "Security" tab to view the Linked Servers. Right click on the linked server (e.g. SIDPERS or RCASDBOR) and select "Properties". On the "Security" tab, you will

see the mappings between SQL Server logins and Oracle logins. You should see "cmsuser" and "sa" mapped to an Oracle login.

NOTE: as mentioned above, you will need to install the Oracle client on the database server and add the appropriate registry keys on the database server in order for the linked servers to function properly.

Configuring Users

Once you the products are installed, you need to start configuring users to access the site. Make sure you are logged into the network with the login you specified in the "Create Admin User" dialog during the CMSWebServices Installation, then use a web browser, go to https://[webservername]/cmswebservices/. You will see a single link to "RCASWeb" which is the user administration. Clicking on this link will bring you to where you can search on users and create new users. Search on your own login, then give yourself permissions to the applications. Once you have given yourself permissions to all the applications, you should see menu options for them in the menu at the top of the page.

To allow other users to access the website, navigate back to the User Administration page with Site Admin->Users->Search off the menu at the top of the page. Selecting the "New" button will bring up a page where you can specify the network login for the user, their unit, link the login to a soldier or Civilian in the database (with the link to the right of the Soldier/Civ), and specify the applications and roles for the user.

The following table gives a brief description of each of the applications and the roles that can be assigned to users:

Application	Role	Description
RCASWeb	Admin	This role allows you to add and configure users into the system. NOTE: The "RCASWeb" application is no longer associated with the AITS system. The TwinEngines applications use security tables that were provided with an earlier version of MILPO Orders which ran on SQL Server.
Discharges	DD214 Clerk	Has access to work with 214s, 215s, and 214 Batches and Templates. Works in the "In Progress" queue.
	DD214 Reviewer	Has access to work with 214s, 215s, and 214 Batches and Templates. Works in the "Ready for Review" queue.
	NGB22 Clerk	Has access to work with NGB-22s. Works in the "In Progress" queue.
	NGB22 Reviewer	Has access to work with NGB-22s. Works in the "Ready for Review" queue.
	Unit Clerk	Has access to the ETS Summary report and the 4836 form.
ETransMgr	ETransMgr User	Has the ability to use all functions within E-Trans Manager.
	ETransMgr Recruiter	Has the ability to view transactions that were sent back to their specific login only. Can alter and change only these transactions.
Awards	Admin	Has the rights to assign what users can publish which awards.
	Awards Publisher	Has the rights to publish awards within the Awards Tracking system. Only has rights to publish awards that have been assigned to them by the Awards Admin.
	Unit Clerk	Has the rights to view eligibility rosters for service awards, create DA638s, and view the Awards for soldiers.
DA21	Admin	NOTE: Not used.
	State Clerk	Has full read/update permissions on all 2-1s that are at or below their assigned organization.
	Unit Clerk	Has view only rights to the 2-1s that are at their assigned organization or below.

MILPOAdmin	MILPO Orders User	Any user that has access to MILPO Orders. This allows them to view reports on their PARs and Orders.
	Transaction Tracking	Has access rights to the Transaction Tracking functionality. This functionality is used to track down electronic transactions created by MILPO Orders that have been amended and revoked and may need to be updated in SIDPERS.
OER	Admin	Has rights to the "Admin" page of OER.
	Intermediate Reviewer	Someone that has reviewing authority prior to being sent to state. For example, a Brigade or Division may need to sign off on all OERs prior to having them sent to state.
	OER Battalion Representative	The person responsible for ensuring that all OERs for their organization get completed and submitted. This person has full access to OERs within their organization.
	OER Rated Officer	Any officer that is rated with an OER. Gives them access to the OER online and the support forms.
	Rater	A person that is rater or intermediate rater for and officer. Gives them access to only parts of the OER that they are responsible for.
	Senior Rater	A person that is a senior rater for any officer. Gives access to OERs in which they are the Senior Rater. Also gives them access to the Senior Rater Profile for themselves and the Senior Rater Calculator.
	Senior Rater Profile Manager	A person that manages the Senior Rater profile for senior raters. They are allowed to view and edit all senior rater profiles within their organization.
	State Clerk	Person responsible at the state level for accepting OERs. Has full access to all OERs.
T&S Tracking	Admin	Has access to the MOS Conversions screen.
	ATRRS Manager	Has access to the "Upload ATRRS Data" to import the data into T&S Tracking. This should be a state level person that can download the ATRRS data from the ATRRS website, then upload the data to T&S Tracking so that the entire state can see the information.
	Training Approval Authority	Not implemented.
	Unit Clerk	Personnel responsible for monitoring training and security within their organization.
NCOER	Admin	Sets the date for which all E5-E9 soldiers are due their NCOER (excluding AGR).
	ncoerUser	A soldier or rater that participates in the evaluations.
	State Clerk	Personnel responsible for tracking NCOERs at the state level.
	Unit Clerk	Personnel responsible for ensuring that NCOERs are completed within their unit. This person has full access to NCOERs within their organization.
Office Admin	Admin	NOTE: Office Admin is no longer used. Do not give rights to this application.
	Local Admin	NOTE: Office Admin is no longer used. Do not give rights to this application.

Synchronization Processes

Under the Site Admin->Data Synchronization, you will find several entries that synchronize data between the TwinEngines products and external systems (e.g. SIDPERS and AITS). These processes will need to be run on a regular basis in order to keep the TwinEngines applications in synch with SIDPERS and AITS. You can run these processes manually by selecting them and clicking on the "Run Selected Synchronization Processes". You can run these processes several times a day.

You can also schedule these stored procedures to run on a regular basis using SQL Server Agent jobs. Use SQL Enterprise Manager to schedule jobs (Management->SQL Server Agent->Jobs). In the CMSWebServices database, you will find a stored procedure called usp_SynchProcesses_Run. This stored procedure will run all of the Synch Processes. Schedule the following SQL to run on an hourly basis during normal business hours:

exec cmswebservices.dbo.usp_SynchProcesses_Run

Make sure SQL Server Agent is started automatically (in Start->All Programs->Administrative Tools->Services) and is using a named account to run the service. The named account that you use for SQL Server Agent will need to have a linked server mapping to the Oracle databases, otherwise you will get authentication errors when running the synchronization processes as part of the scheduled job.

NOTE: It is TwinEngine's intention that these "Data Synchronization" processes will eventually take the place of the loader and we will no longer import data via the loader. Not all of our applications, however, have been converted over to pulling data directly from SIDPERS and AITS, so you will still need to run the loader on a regular basis. Most importantly, the organizational structure that is the key to the security of the applications is still being pulled from the data that is imported as part of the loader.

Application Specific Installation Notes

NCOER
After the installation, go to the NCOER Release Notes menu option and follow the "Getting Started Guide" link. This will give you information about setting up your default end of evaluation period dates and setting up rating schemes.

Discharges
Part of the "Data Synchronization" processes will create NGB-22's from Discharge orders created in MILPO Orders. Running this process will generate 22s on all Discharge and Separation orders created in MILPO Orders.

DA2-1
You will need to configure reference tables for Awards, Campaigns, Weapons Types, and MOS Titles. Use the Site Admin->Reference Tables menu options to configure these tables. The Awards table will need your state awards as well as any abbreviations that are used on the 2-1.

OER
You will need to create or import your Senior Rater profile history into the system before you can take advantage of the automatic COM calculations. You can request the data from NGB, then import it into the database tables, but you will still need to review the data for accuracy and completeness.

A batch file has been installed on the web server called oer_import.bat in the Program Files\OER\Import NGB Data directory. This batch file will use the SQL Server BCP utility to import the tables into the database. Since it uses BCP, you will have to run the import on the SQL Server.

E-Trans Manager

Part of the "Data Synchronization" processes copies electronic transactions from MILPO Orders over to E-Trans Manager. The transactions are not deleted from MILPO Orders, just copied to the E-Trans database. See the E-Trans Manager user's guide for more information about running E-Trans Manager.

Training & Security Tracking

Part of the "Data Synchronization" processes handles determining what soldiers are considered Duty MOS Qualified and what soldiers are not.

In order to view the list of documents that have been put into PERMS, you must import the PERMS data into the CMSWebServices database table, doc_data. NGB can send you an export of the PERMS data on a regular basis. When you receive this data, place it on the SQL Server box, then use SQL Server's Data Transformation Services (DTS) to import the data. A DTS package called Import PERMS doc_data.dts has been installed for you in the Program Files\TrainingTracking directory on the web server. To run this DTS, do the following:

1. In SQL Enterprise Manager, right click on "Data Transformation Services" and select "All Tasks->Open Package".
2. Locate the "Import PERMS doc_data.dts" DTS package.
3. Double-click on the doc_data text file icon
4. Change the "File Name" to point to the file NGB sent you.
5. Select "No" when prompted "Do you want the transformations that have been defined using this connection to be reset?"
6. Select "Package->Execute" from the menu options.
7. After the import has run, select "Package->Save As"
8. Change the "Location" to "SQL Server"

Once the package is saved, you can schedule it to run on a regular basis. This is helpful if you want to automatically import the file at a specific time. This way when you receive the file, you can just replace the existing file and let the scheduled DTS task import it the next time it runs. To schedule the package, expand "Data Transformation Services", select "Local Packages", then right click on the "Import PERMS doc_data" package and select "Schedule".

To import your ATRRS information, you must download the spreadsheets from the AFAMM website and save them in a "Comma Separated Values" (csv) format. Use the Upload ATRRS Data screen to import the data into the system.

Upload Directories and End-User Permissions

Some of the applications allow the end user to upload files to the web server. In order to upload files to the web server, you must give the end-user write permissions to the upload folders. These folders include:

Application	Directory	Description
CMSWebServices	CMSWebServices\Web\PERMSUploads	Used to upload the PERMS doc_data information and import. The PERMS doc_data is used by both Discharges and T&S Tracking. Only the RCASWeb "Admin" users will need write permissions to this folder.
E-Trans Manager	ETransMgr\Web\ETMUploads	NPSG and PSG transaction files are uploaded to this location. Anyone that imports the NPSG and PSG transactions to this directory will need write permissions.
T&S Tracking	TrainingTracking\Web\Uploads	The ATRRS Manager uploads the ATRRS data here. Anyone performing the "Upload ATRRS Data" function will need write permissions to this folder.

Performing Upgrades

When upgrading your applications, always be sure to upgrade CMSWebServices to the latest release as well. This product contains shared components for all the applications and may have added features that the newer products require.

Be sure to back up your existing databases (CMS, CMSWebServices, Discharges, DA21, NCOER, etc.) before beginning the upgrade process.

When upgrading your products to a new version, you must first uninstall the previous version. Use "Add Remove Programs" to uninstall the products you are upgrading. Once the all the products are uninstalled, start with the CMSWebServices installation, then proceed with the product installations.

You will be prompted for the SQL Server Administrator login information in order for the installation program to upgrade your database.

Additional Help

Additional help is available from the TwinEngines portal at: http://sharepoint.twinengines.com/NG. The "Issue Tracking" link to the left (http://sharepoint.twinengines.com/NG/Lists/Issue%20Tracking/AllItems.aspx) has a list of common problems that you can run into. You can search through the site for issues using the search text box in the upper right hand corner of the page.

Email support is available through: ngsupport@twinengines.com.

Pre-Installation Checklist

☑	Task	Notes
	Microsoft Web Server Identified (Win 2000 or 2003)	
	• Administrative rights to install software	
	• Network DTC enabled	
	• SSL Certificate Installed	
	Microsoft SQL Server Identified (SQL 7 or 2000)	
	• SQL Server administrative rights to build databases, create users	
	• Oracle Client Installed on database server	
	• Oracle SQL*Net Alias created for RCASDBOR and SIDPERS	
	• SQL Server Agent service set to start automatically and running as a named account	
	• Application Databases Created	
	• SQL Server and Windows Authentication allowed (SQL Enterprise Manager->Properties->Security – make sure the "SQL Server and Windows" is selected under "SQL Server provides authentication based on Windows accounts and a named SQL Server login ID and password.")	
	Network account identified for applications	
	• "Power User" rights on the web server.	
	• Logon as a Batch Job rights granted on web server	
	• Logon as a service rights on web server	
	Oracle login identified for access to SIDPERS	
	• Read access on SIDPERS tables	
	Oracle login identified for access to AITS database	
	• Access permissions granted to Oracle AITS login (see section below)	
	FTP Login to access UPS extract files on SIDPERS	

Post-Installation Checklist

☑	Task	Notes
	On the Database Server	
	• Compare UPS extract filenames from SIDPERS to cms.dbo.tblImportRef to ensure file names match	
	• Add Oracle Registry keys (Oracle_9.reg, Oracle_8_1.reg, or Oracle_8_0.reg) found in the CMSWebServices installation directory to the SQL Server system and reboot SQL Server	
	• Add the SQL Server Agent Identity to the linked server login mappings so that the SQL Server Agent can run scheduled tasks which pull data from AITS and SIDPERS	
	• Schedule cmswebservices.dbo. usp_SynchProcesses_Run to periodically run (e.g. hourly) procedures which pull data from SIDPERS and AITS	
	• Schedule a regular backup of all databases.	
	On the Web Server	
	• Use "Create Admin User" under the CMSWebServices menu options to create initial Admin user that will be used to configure additional users	
	• Run CMSWebServices loader	
	From any web browser	
	• Use Site Admin to configure additional user access	
	• Add State Awards to Site Admin->Reference Tables	
	• Under Site Admin->Configuration, set the MILPO Orders Version to 8+ and the MILPO Orders Server to the name of the AITS **web** server	