

Setup and Maintenance Guide



Merge, Manage, & Modernize E-Learning Development

Table of Contents

1	Introduction	5
2	Server STIGs.....	5
3	System Requirements.....	5
4	DoD SSL certificates	6
4.1	<i>Obtaining DoD SSL certificates.....</i>	6
4.1.1	Import DoD Web Server Certificate or SMTP certificate	6
4.2	<i>Installing your own Certificate Authority.....</i>	7
4.2.1	Install Active Directory Certificate Services	7
4.2.2	Generate Web Site Certificate Request	8
4.2.3	Generate SMTP Certificate Request	17
4.2.4	Generate SQL Certificate Request	19
4.2.5	CA Root Certificate.....	20
5	Install DoD root certificates with InstallRoot (Web Server)	20
5.1	<i>Verify InstallRoot installed successfully.....</i>	20
6	Setup Windows Roles and Features on the Web Server.....	21
7	.NET Framework 4.8 (Web Server)	24
8	File System (Web Server)	24
8.1	<i>Folder Copies.....</i>	24
8.1.1	MELD Directory	24
8.1.2	IME_Data.....	25
8.2	<i>Folder Permissions</i>	25
8.2.1	Inetpub	25
8.2.2	MELD/IME/Web.config.....	25
8.2.3	MELD/global.asa	25
8.2.4	Additional Folder Permissions.....	26
9	Configure MELD website for SSL	27
9.1	<i>Edit Binding</i>	27
9.2	<i>Enable Client Certificate Negotiation.....</i>	28
9.3	<i>Require SSL and Client Certificates.....</i>	30
9.4	<i>Update Logging.....</i>	30
10	Enable HSTS on MELD website	31
11	Create MELD Application (IIS).....	32
11.1	<i>Enable Parent Paths (IIS).....</i>	34

11.2	<i>Error Browser Settings</i>	35
11.3	<i>Create IME Application (IIS)</i>	35
11.3.1	Setup uploadreadAheadSize	36
11.3.2	Create IME Data Virtual Directories (IIS).....	37
11.4	<i>Application pool settings</i>	39
11.4.1	Update application pool recycling options	39
11.4.2	Update application pool identity	40
11.4.3	Increase Session Timeout (IIS)	41
11.5	<i>URL Rewrite</i>	42
11.5.1	Install	42
11.6	<i>MIME types</i>	42
12	SQL Server	43
12.1	<i>Microsoft SQL Server Management Studio</i>	43
12.2	<i>Server Authentication</i>	43
12.3	<i>SQL Server Management Studio</i>	43
12.3.1	Copy Databases	43
12.3.2	Create EXEC role	44
12.3.3	Create MELD SQL Server Account	44
12.3.4	Set Password Dates.....	46
12.3.5	Additional SQL Server Accounts.....	46
12.4	<i>Install OLE DB Driver for SQL Server</i>	46
12.5	<i>Update SQL encryption</i>	46
13	Update Configuration Files within MELD (File System)	47
13.1	<i>Global.asa</i>	47
13.1.1	Connection Strings	47
13.1.2	Application Physical Path	48
13.1.3	QASP_Option	49
13.1.4	DoD Settings	49
13.2	<i>MELD\IME\Web.config</i>	51
13.2.1	Update Connection Strings	51
13.2.2	Encrypt Connection String.....	52
13.2.3	Update Additional Settings	52
14	Setup SMTP on Web Server	53
14.1	<i>Set Service to Automatic</i>	53
14.2	<i>Open Port</i>	53
14.3	<i>mailroot permissions</i>	53
14.4	<i>McAfee Settings</i>	53
14.5	<i>Launch IIS 6 (installs when the SMTP feature is added)</i>	55
14.5.1	Require TLS encryption.....	55

14.5.2	Set Relay Servers.....	56
15	Launching MELD.....	56
15.1	<i>Initial Launch.....</i>	56
15.1.1	Smart Card Systems.....	56
15.1.2	Username / Password Systems.....	60
15.2	<i>Project Selection.....</i>	63
15.3	<i>Browser Support.....</i>	63
15.4	<i>User Guides.....</i>	63
16	System Backups.....	64
16.1	<i>File System.....</i>	64
16.2	<i>SQL Server Backups.....</i>	64
16.2.1	SQL Full Version.....	64
16.2.2	SQL Express.....	65
17	MELD System Maintenance and Security Plan.....	73
17.1	<i>Receiving packages from MELD Support.....</i>	73
17.1.1	Update/Installation Package Verification.....	74
17.2	<i>File Server Resource Manager.....</i>	74
17.2.1	IME_Data quota.....	74
17.2.2	InetPub folder quota.....	77
17.2.3	SQL Server data folder quota.....	77
17.2.4	Enable SMTP.....	77
17.3	<i>SQL Server Security Plan.....</i>	78
17.3.1	Authorized Users.....	78
17.3.2	Testing Database Recovery.....	78
17.3.3	Updating password for meld_user.....	79
17.4	<i>IIS Security Plan.....</i>	80
17.4.1	DISA revocation lists.....	80
17.4.2	Web Server Certificate Renewal.....	81
17.4.3	Off load IIS Log Files.....	81
17.4.4	Audit Configuration Files.....	81
17.5	<i>Log Folder Maintenance and Rollover.....</i>	83
17.5.1	Daily Review.....	83
17.5.2	MELD Update Log Folder Review and Rollover.....	83
17.5.3	MELD Audit Log Failures.....	84
17.6	<i>MELD Account Alerts.....</i>	84
17.7	<i>Resuming MELD after a System Failure.....</i>	84
17.8	<i>Shutting Down MELD in the Event of an Attack or Unauthorized Update.....</i>	84
17.8.1	Immediate Shut down.....	84
17.8.2	Disaster Recovery.....	85

17.9 *Troubleshooting Errors on Web Server* 85

 17.9.1 Failed Request Tracing 85

 17.9.2 Submitting Log files from Web Server 87

17.10 *Submitting Defects*..... 88

18 Log Browser **88**

 18.1 *MELD Audit Logs* 88

 18.2 *IIS Audit Logs* 89

 18.3 *Accessing the Log Browser*..... 89

 18.4 *Read Log Events*..... 91

 18.4.1 Basic Filters..... 91

 18.4.2 Detailed Filters 92

 18.4.3 Event Listing 92

 18.4.4 Report 94

 18.5 *Audit File Tampering* 96

19 Sandbox Install..... **97**

1 Introduction

MELD is a server side intranet application utilizing classic ASP, .NET Framework 4.8, and SQL server databases. This guide will provide instructions for setting up and maintaining the MELD application on a web server.

2 Server STIGs

Before configuring MELD ensure the server meets all the DoD STIG requirements. Please consult your project manager for detailed server requirements.

MELD was designed following the current version of the DoD Application Security and Development Security Technical Implementation Guide. However, it is important to understand what DoD requirements are for your system before proceeding with this setup. For instance some standalone systems may not require CAC credentials and may not have to follow the same DoD requirements as a system available over the Internet. It is recommended to first read this entire guide completely and then contact your project manager to determine if your site has any unique system requirements.

3 System Requirements

Component	Requirement
Hard Disk	<ul style="list-style-type: none"> 10 GB of available hard-disk space (C drive) An additional hard drive with 100GB to support storing the courseware files (this drive depends on the size and amount of courseware). <p><i>*for standalone desktop instances the same drive can be used for both if an additional drive is</i></p>

	<i>not available</i>
Memory	8GB or more
Processor Speed	2.0 GHz or faster
Operating System	Desktop: Windows 10 Server: At least Windows Server 2012

4 DoD SSL certificates

Before MELD can be configured on the server, a DoD approved SSL certificate will need to be obtained for the web site as well as the SMTP service. If the MELD web server is a DoD registered server, the DoD can provide these certificates.

In certain standalone instances where obtaining a DoD assigned SSL certificate may not be possible, the DoD may approve of installing a Certificate Authority on the domain server to issue the required SSL certificates.

Contact your project manager to determine how to proceed. If the project manager determines that the DoD will provide the certificates then proceed to step 4.1. If obtaining a DoD certificate is not possible then proceed to step 4.2.

4.1 Obtaining DoD SSL certificates

The DoD will provide instructions for obtaining a DoD certificate. Follow the DoD instructions to obtain the certificates as well as the instructions for installing the certificates on the server.

You will need the following information to request the SSL web site certificate:

- The **fully qualified domain name** for the MELD web server. To find the fully qualified domain name for the web server, select Control Panel> System and Security>System. The fully qualified domain name will be listed under Full Computer Name. This is typically attached to a field title "Subject Name / Common Name"
- The **alternative names** for the MELD web server. The alternative names will include the name of the web server (not the full name) as well as the IP address of the web server. This is typically attached to a field titled "Alternative names / DNS". Modern browsers require that alternate names are listed within the SSL certificate and will produce certificate trust errors if they are not provided.

For the SMTP certificate only the fully qualified domain name should be used. Alternative names should not be used for the SMTP certificate.

4.1.1 Import DoD Web Server Certificate or SMTP certificate

1. Run the Microsoft Management Console by entering MMC in the search bar and then launching it.
2. Select File>Add/Remove Snap in...
3. Select Certificates in the left column and then select the Add button.
4. Select Computer Account.
5. Select Local Computer.
6. Select Finish and then select OK.
7. The Certificates snap in should now be loaded. Right-Click on Personal under Certificates (Local Computer) and select All Tasks>Import to import the DoD Web Server Certificate.

Note: The console window can be saved with the certificate Snap in to skip the above steps when accessing at a later time.

Important: *The web server certificate needs to be placed in the Personal folder. These certificates cannot be placed into the Trusted Root Certification Authorities location. The Trusted Root Certification Authorities location is reserved only for Root CAs and IIS will fail to authenticate client certificates if any personal or immediate certificate is placed in the trusted root location.*

4.2 Installing your own Certificate Authority

Note: Only use this method if obtaining an SSL certificate from the DoD is not possible and the DoD has approved installing a certificate authority on the MELD standalone network.

The Certificate Authority should be installed on a permanent server within your domain. In smaller networks this can be installed on your domain controller.

The default Microsoft install can be used to install Active Directory Certificate Services and can be accessed from this URL: <https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority>

The steps are also listed below for easier access:

4.2.1 Install Active Directory Certificate Services

Important steps before install:

- Before you install Active Directory Certificate Services, you must name the computer, configure the computer with a static IP address, and join the computer to the domain. For more information on how to accomplish these tasks, see the Windows Server 2016 [Core Network Guide](#).
- To perform this procedure, the computer on which you are installing AD CS must be joined to a domain where Active Directory Domain Services (AD DS) is installed.

Install Steps:

1. Log on as a member of both the Enterprise Admins group and the root domain's Domain Admins group.
2. In Server Manager, click **Manage**, and then click **Add Roles and Features**. The Add Roles and Features Wizard opens.
3. In **Before You Begin**, click **Next**.
Note : The **Before You Begin** page of the Add Roles and Features Wizard is not displayed if you have previously selected **Skip this page by default** when the Add Roles and Features Wizard was run.
4. In **Select Installation Type**, ensure that **Role-Based or feature-based installation** is selected, and then click **Next**.
5. In **Select destination server**, ensure that **Select a server from the server pool** is selected. In **Server Pool**, ensure that the local computer is selected. Click **Next**.
6. In **Select Server Roles**, in **Roles**, select **Active Directory Certificate Services**. When you are prompted to add required features, click **Add Features**, and then click **Next**.
7. In **Select features**, click **Next**.
8. In **Active Directory Certificate Services**, read the provided information, and then click **Next**.
9. In **Confirm installation selections**, click **Install**. Do not close the wizard during the installation process. When installation is complete, click **Configure Active Directory Certificate Services on the destination server**. The AD

August 1, 2021

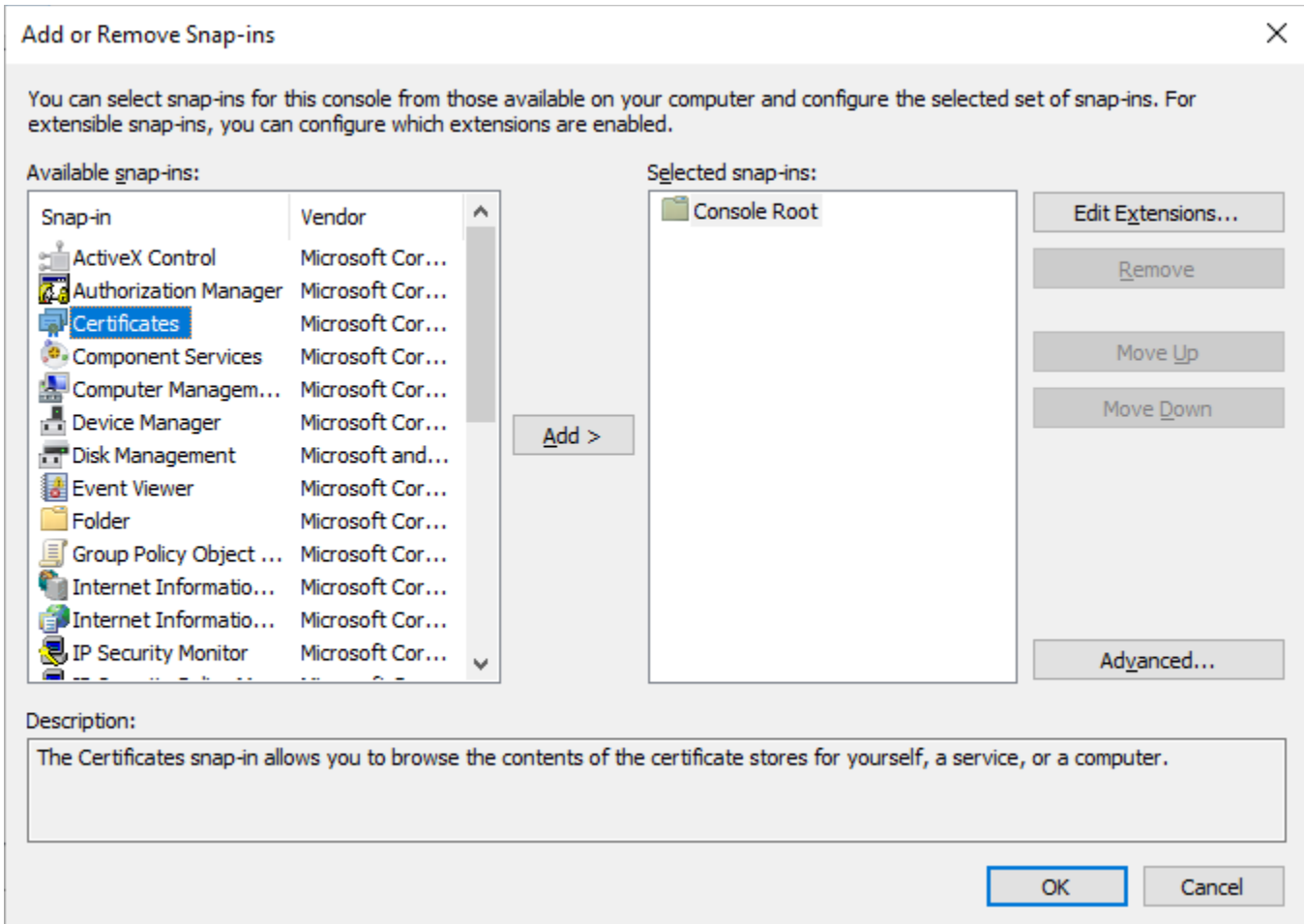
CS Configuration wizard opens. Read the credentials information and, if needed, provide the credentials for an account that is a member of the Enterprise Admins group. Click **Next**.

10. In **Role Services**, click **Certification Authority**, and then click **Next**.
11. On the **Setup Type** page, verify that **Enterprise CA** is selected, and then click **Next**.
12. On the **Specify the type of the CA** page, verify that **Root CA** is selected, and then click **Next**.
13. On the **Specify the type of the private key** page, verify that **Create a new private key** is selected, and then click **Next**.
14. On the **Cryptography for CA** page, keep the default settings for CSP (**RSA#Microsoft Software Key Storage Provider**) and hash algorithm (**SHA2**), and determine the best key character length for your deployment. Large key character lengths provide optimal security; however, they can impact server performance and might not be compatible with legacy applications. It is recommended that you keep the default setting of 2048. Click **Next**.
15. On the **CA Name** page, keep the suggested common name for the CA or change the name according to your requirements. Ensure that you are certain the CA name is compatible with your naming conventions and purposes, because you cannot change the CA name after you have installed AD CS. Click **Next**.
16. On the **Validity Period** page, in **Specify the validity period**, type the number and select a time value (Years, Months, Weeks, or Days). The default setting of five years is recommended. Click **Next**.
17. On the **CA Database** page, in **Specify the database locations**, specify the folder location for the certificate database and the certificate database log. If you specify locations other than the default locations, ensure that the folders are secured with access control lists (ACLs) that prevent unauthorized users or computers from accessing the CA database and log files. Click **Next**.
18. In **Confirmation**, click **Configure** to apply your selections, and then click **Close**.

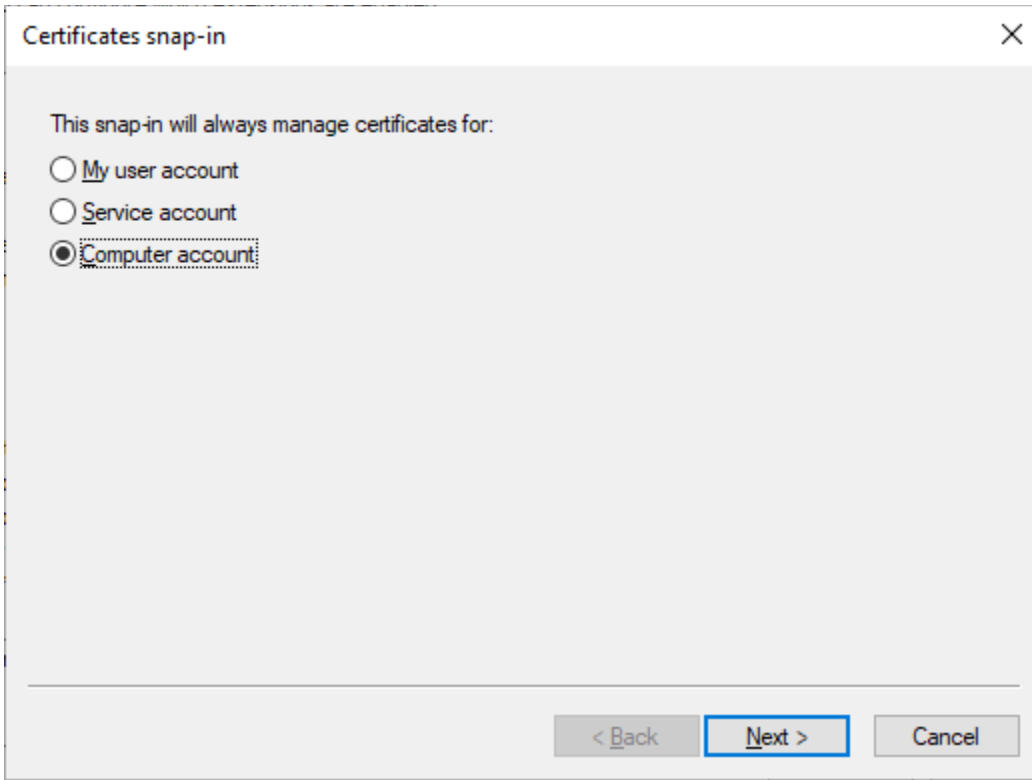
4.2.2 Generate Web Site Certificate Request

After the Certificate Authority is setup in the previous step, you will need to create the certificate request for the website.

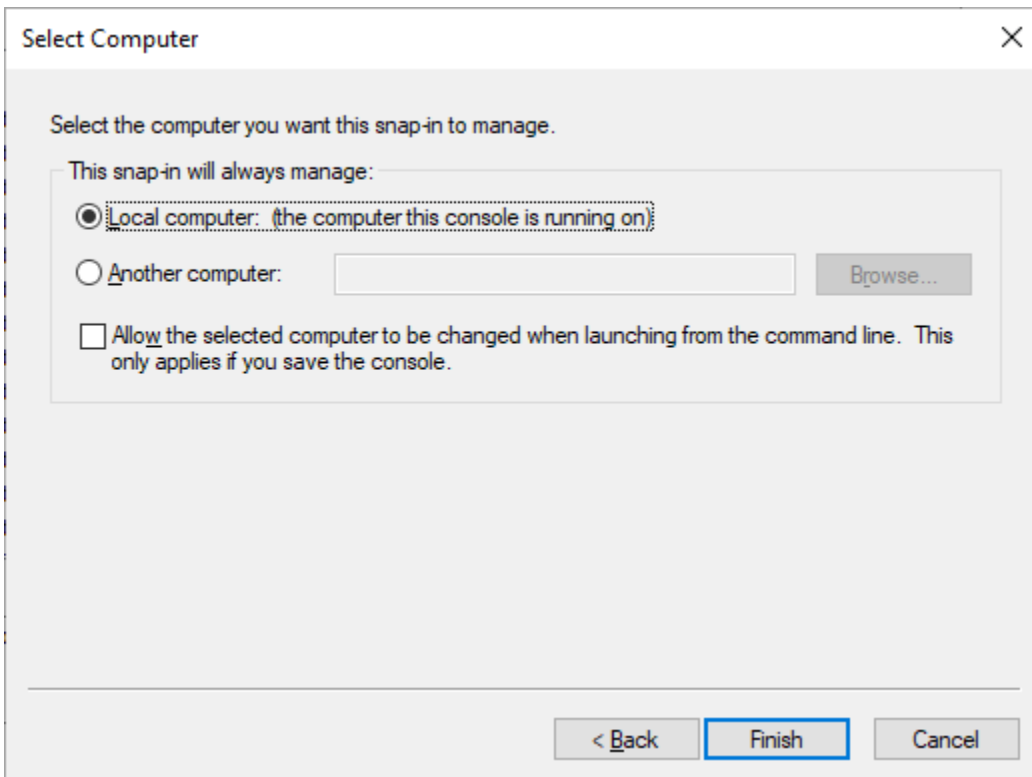
1. Login to the web server. This most likely will not be the same server the Certificate Authority was previously setup on.
2. Run the Microsoft Management Console by entering **MMC** in the search bar and then launching it.
3. Select **File>Add/Remove Snap in...**
4. Select **Certificates** in the left column and then select the **Add** button.



5. Select **Computer Account**.



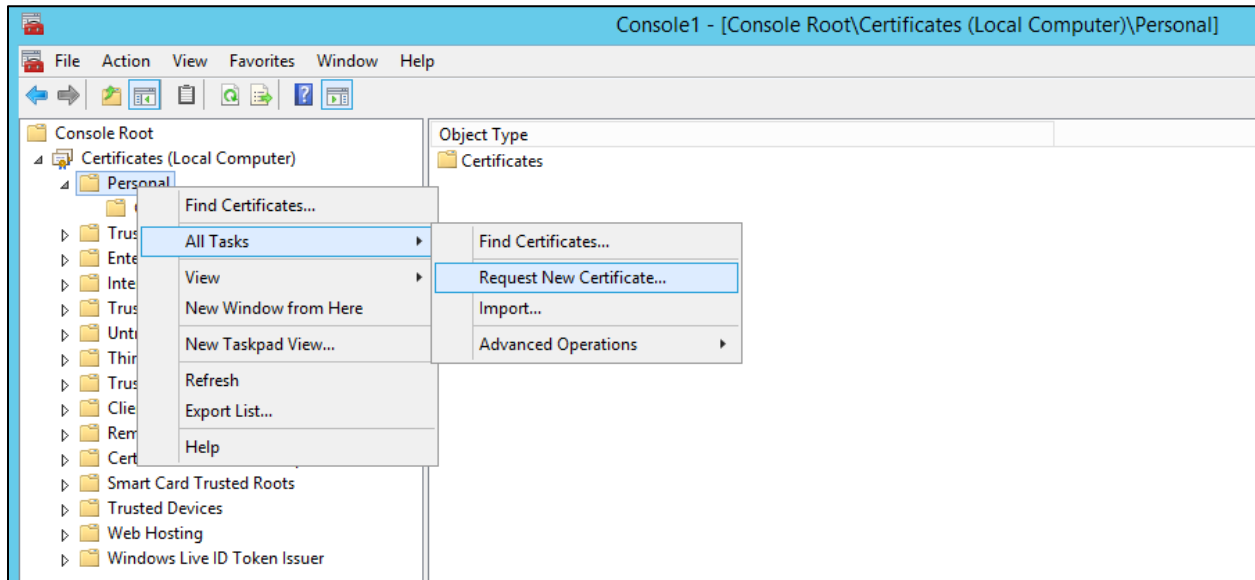
6. Select **Local Computer**.



7. Select **Finish** and then select **OK**.

August 1, 2021

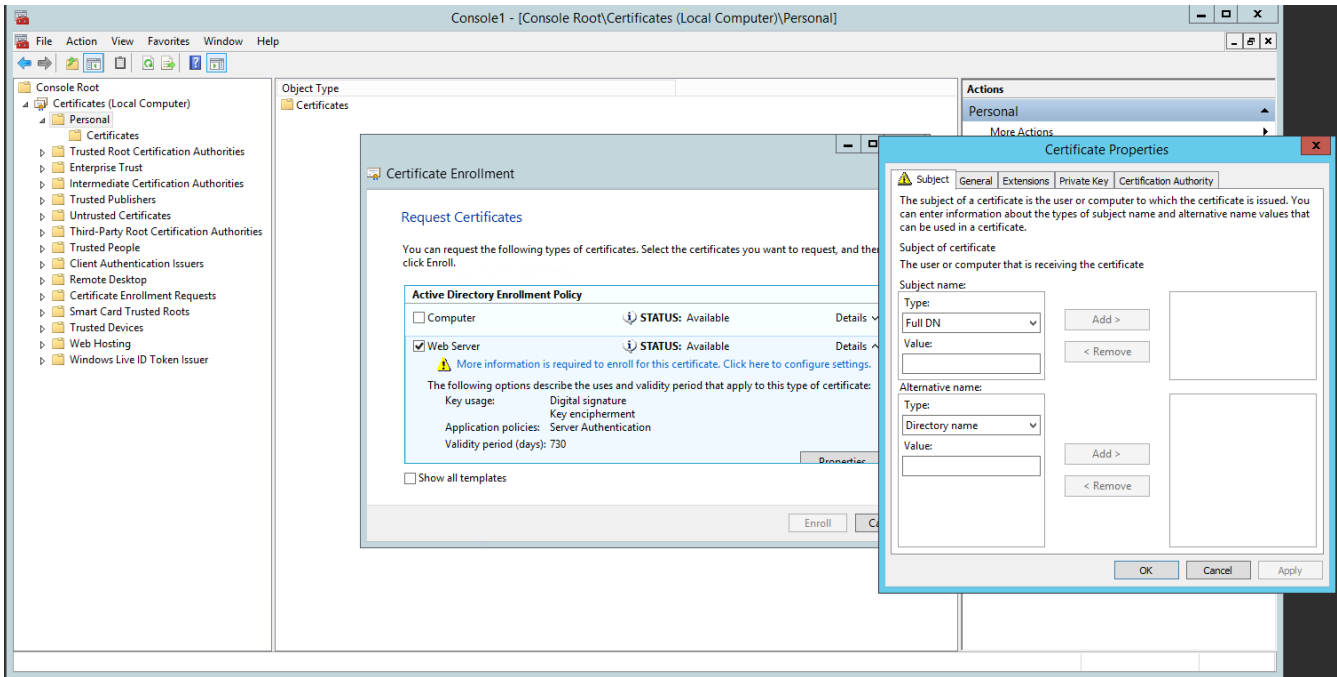
8. The **Certificates** snap in should now be loaded. Right-Click on **Personal** under **Certificates (Local Computer)** and select **All Tasks>Request New Certificate**.



9. Select **Next**.
10. Select **Next Again**.
11. Select **Web Server**.

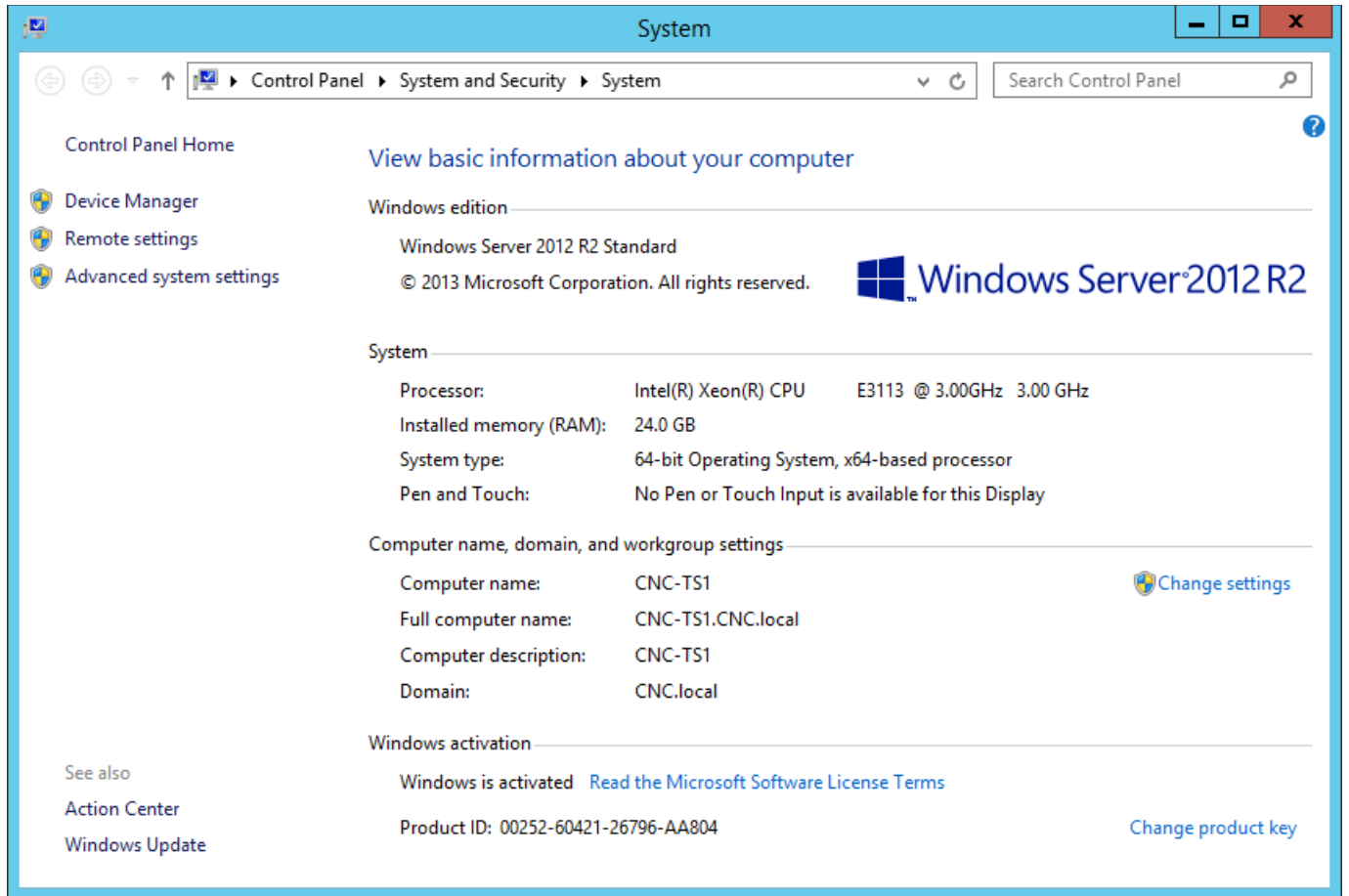
Note: If the Web Server template does not show up in the list, then the logged in user does not have permissions to enroll in the certificate. To allow the signed in user to Enroll, an administrator will need to login to the domain server (or the server the certification services was installed on) and follow the below steps:

- a) From Administrator Tools>Run the **Certificate Authority**.
- b) The CA will be listed. Right click on **Certificate Templates** and select **Manage**.
- c) Locate the web server template, right click and then select **Properties**.
- d) Navigate to the **Security** tab and then add the necessary users to give **Enroll** permissions. *Note: You may need to grant "Authenticated Users" enroll permissions if individual accounts continue to not allow enrollment.*
- e) Select **OK** when complete.



12. Click on the **More Information is required** warning. On the **Subject** tab enter the following,
 - a) Under **Subject name**, select the **Type** drop down and select **Common Name**. Type the fully qualified domain name for this web server and then select **Add**. *Note, this is very important that the fully qualified name is entered.*

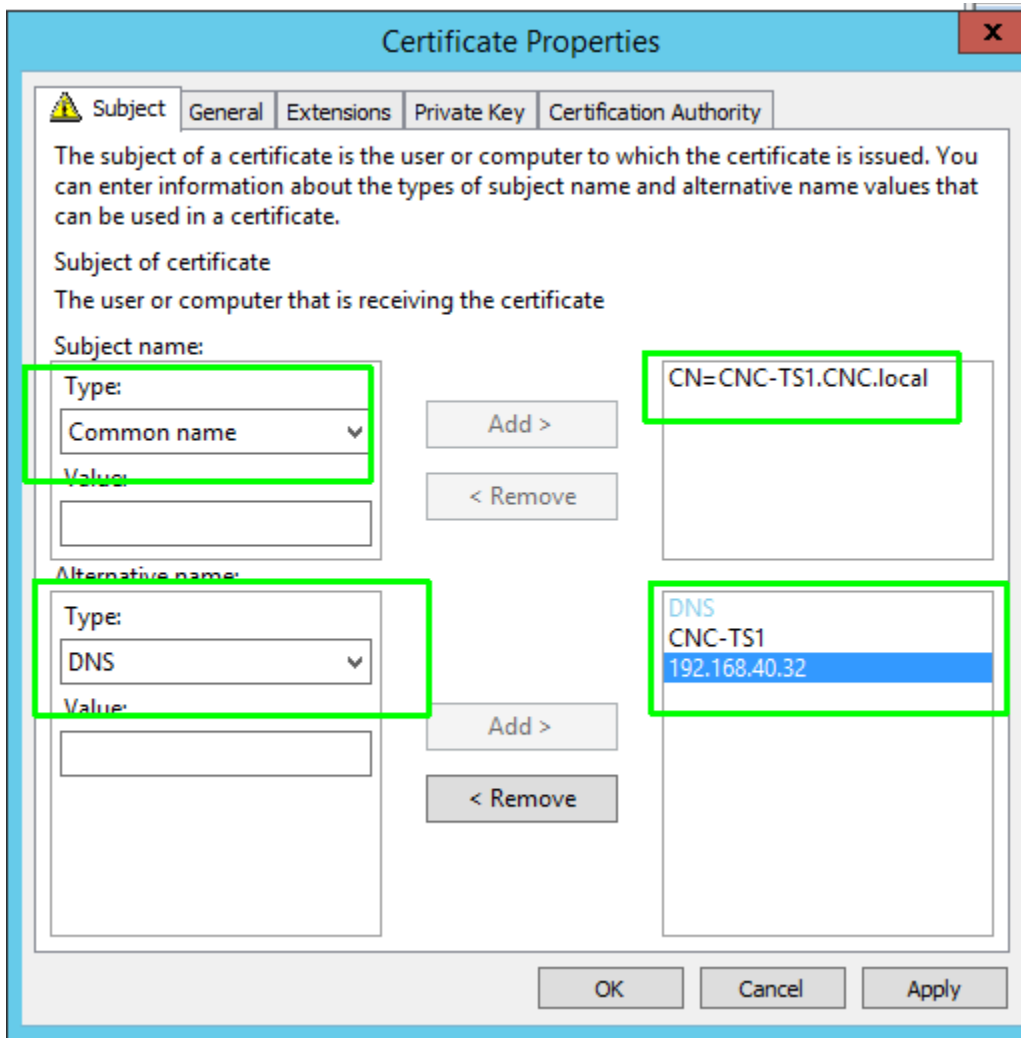
*Note: to find the fully qualified domain name for this web server, Select **Control Panel> System and Security>System**. The fully qualified domain name will be listed under **Full Computer Name**.*



- b) Under **Alternative name**, select **DNS** and then enter the following:
- Server name
 - IP address
 - If host names are used for the web application, then all host names will need to be added as well. Refer to the DNS lookup for a list of all host names. An example of a host name is MELD, where a user would access the site as `https://MELD`

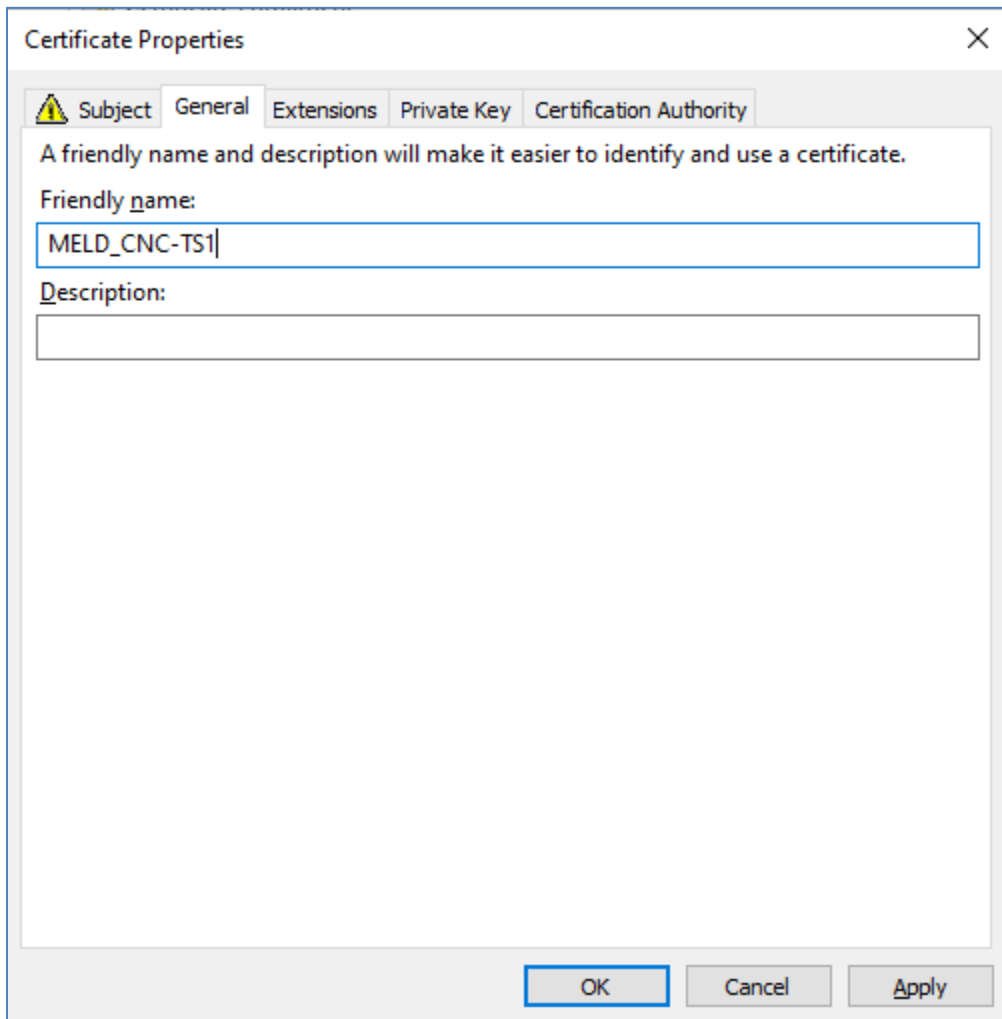
Select the **Add** button for each.

Note: You must enter the Alternative Names and not skip this step. Chrome and other modern browsers will produce certificate error warnings if not entered.

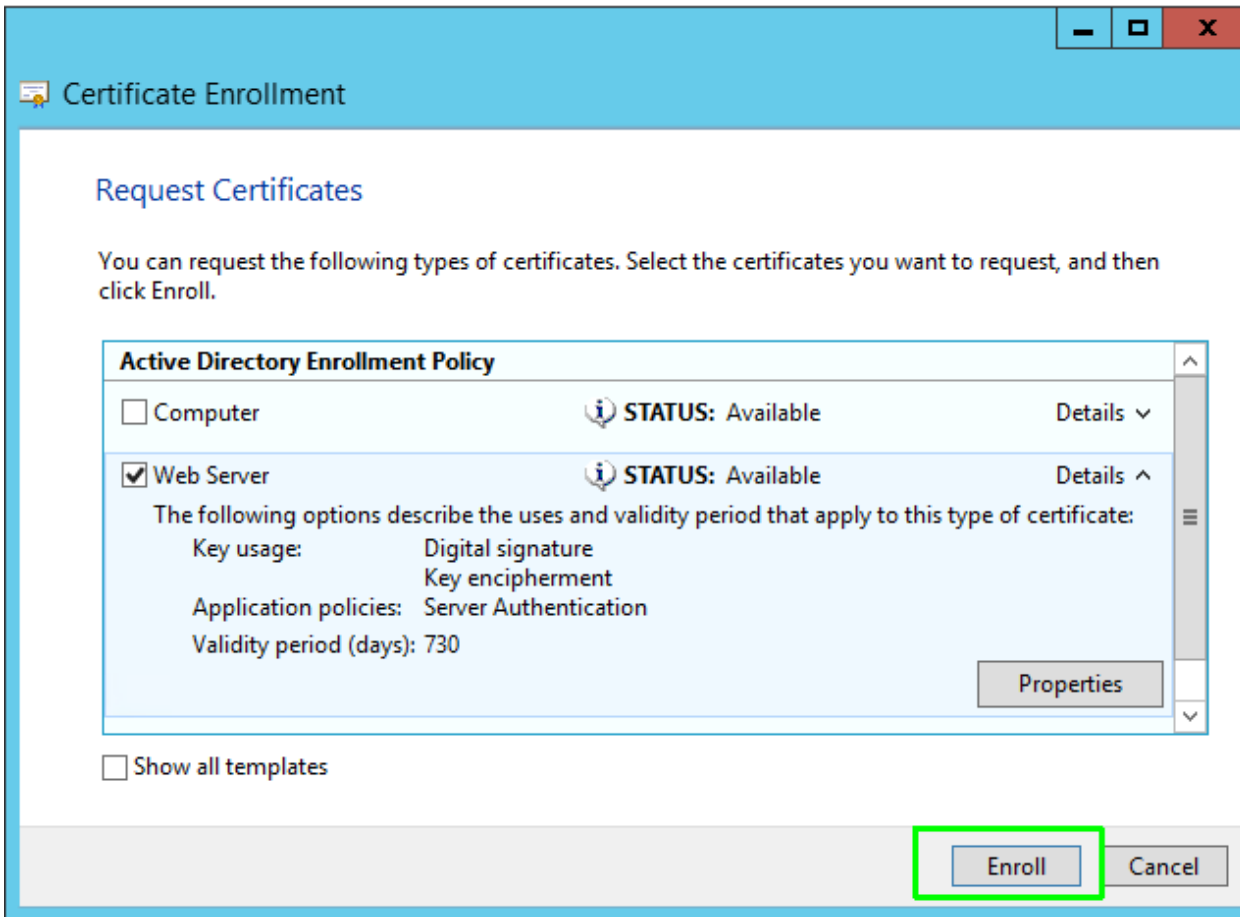


13. Under the **General** tab enter a friendly name so this certificate can be easily identified later within IIS.

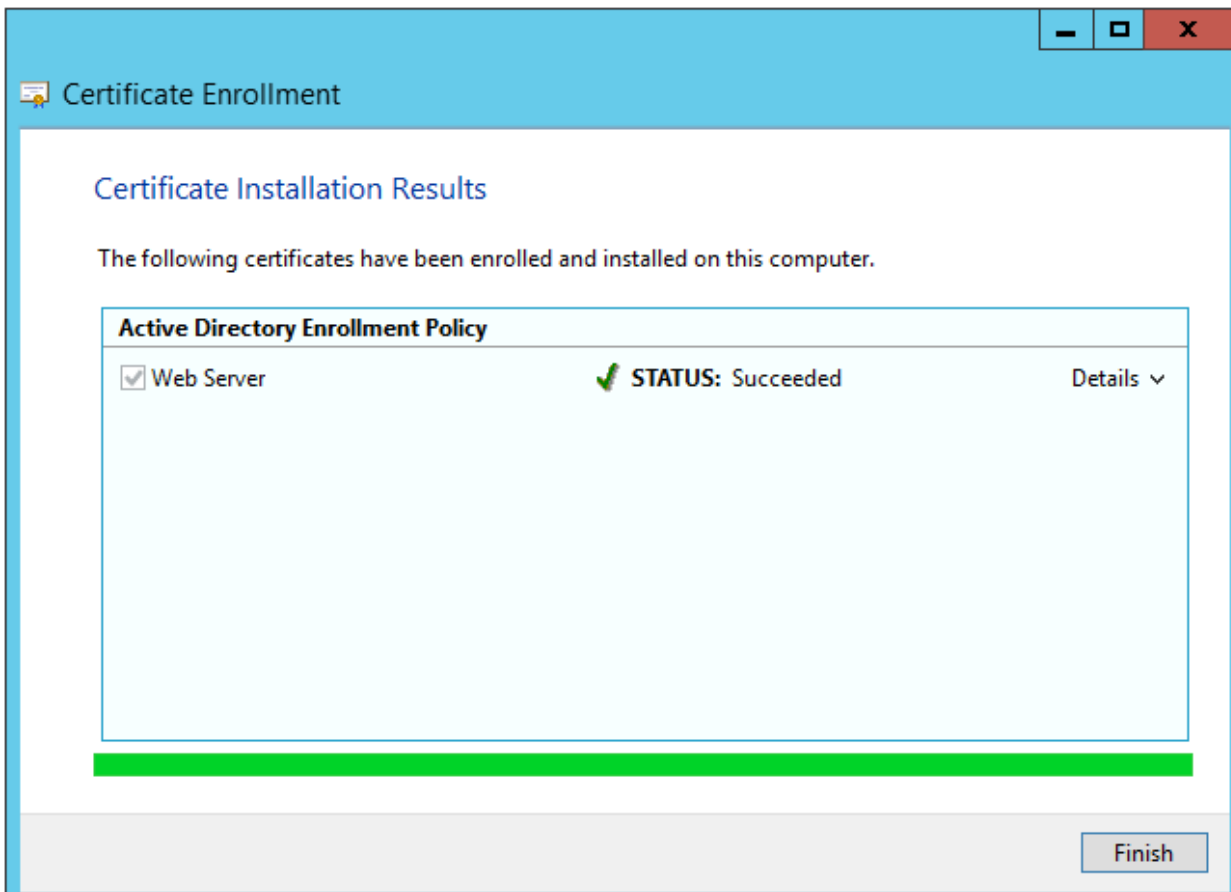
August 1, 2021



14. Under the **Certificate Authority** tab , ensure the correct certificate authority is selected. If multiple exists on the domain, then you will need to select the desired one. If any orphaned records exist from prior certificate authorities, ensure those are not selected to prevent enrollment errors.
15. Select **OK** to close the Certificate Properties window.
16. Select the **Enroll** button from the main Certificate Enrollment window.



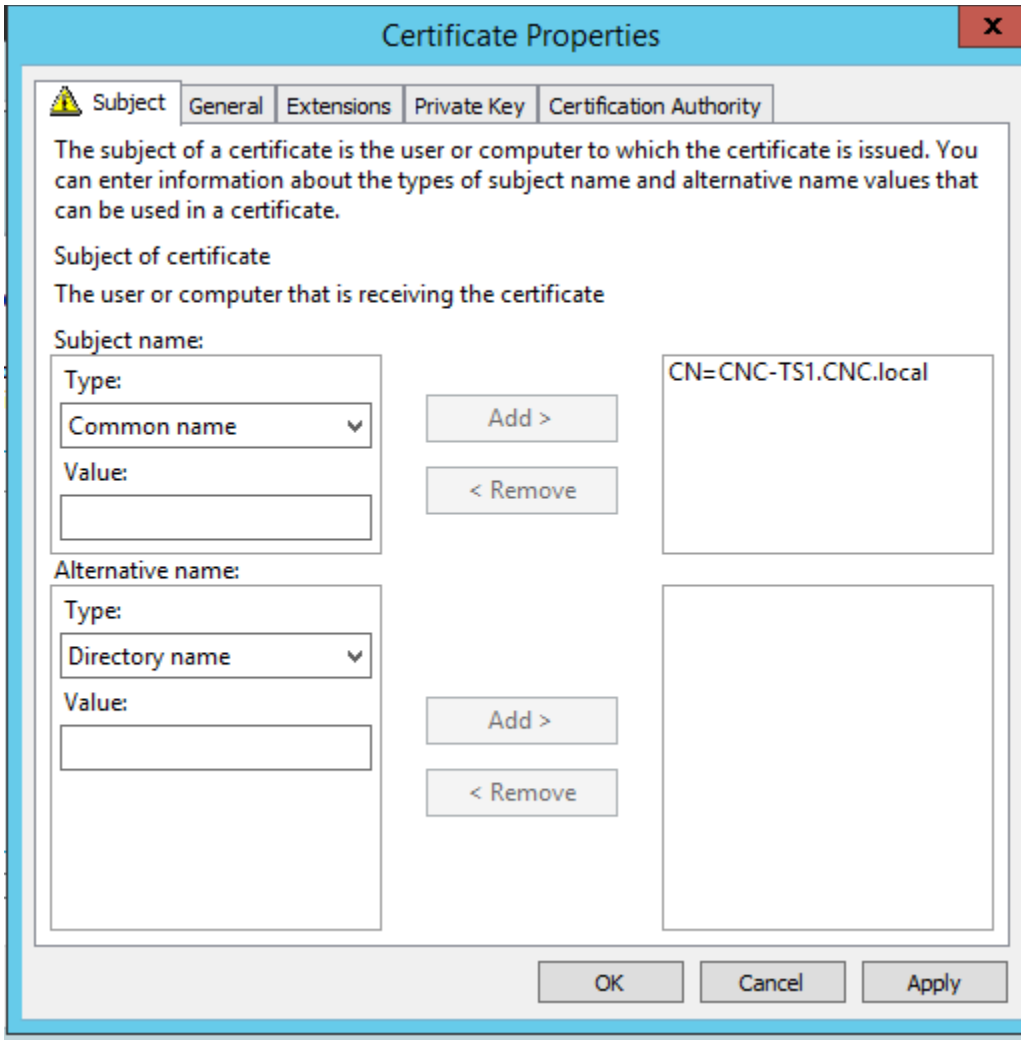
17. Select the **Finish** button from the main Certificate Enrollment window.



4.2.3 Generate SMTP Certificate Request

Follow the same steps in the above section, with the following exceptions:

1. Do not setup **Alternate Names**. The SMTP service will not recognize a certificate with alternative names.
2. On the general tab, use a different friendly name to identify the certificate.



Certificate Properties [X]

Subject | General | Extensions | Private Key | Certification Authority

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate
The user or computer that is receiving the certificate

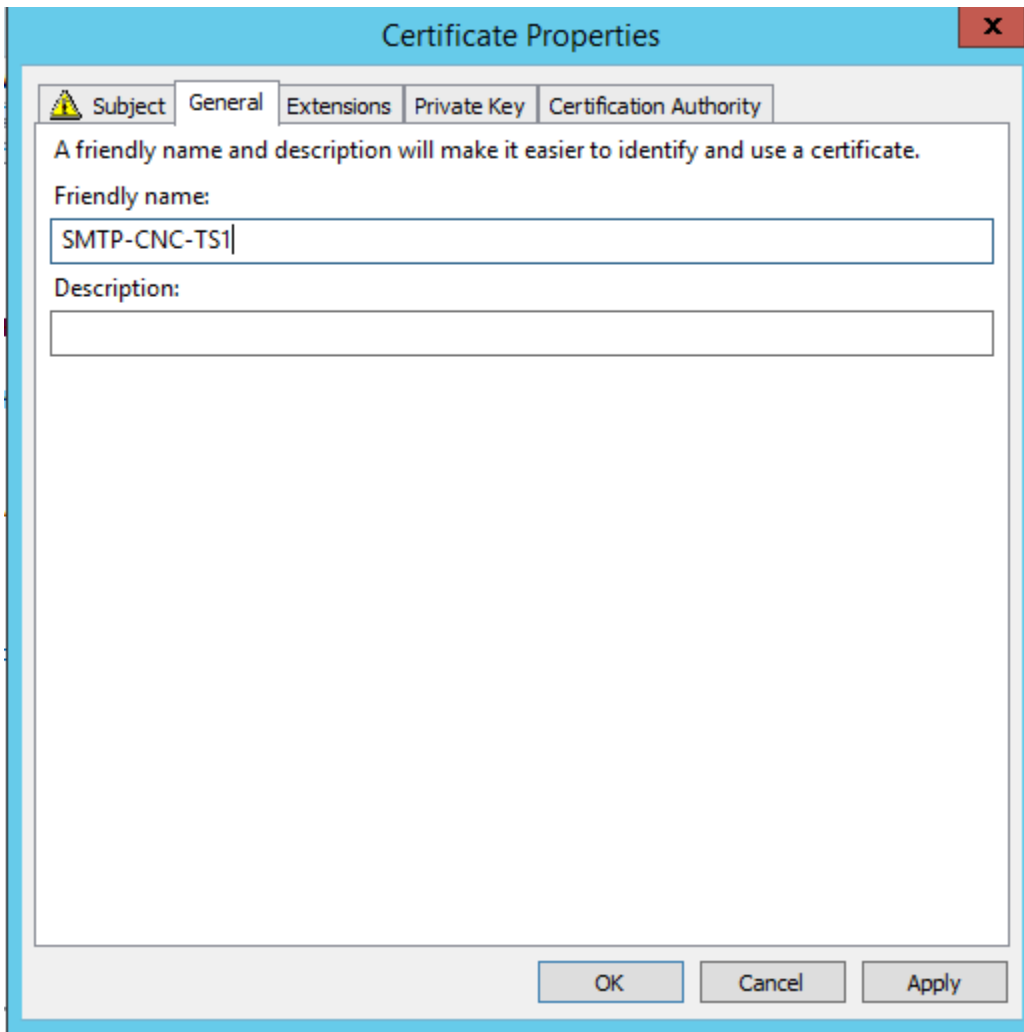
Subject name:

Type: Common name	Add >	CN=CNC-TS1.CNC.local
Value: []	< Remove	

Alternative name:

Type: Directory name	Add >	[]
Value: []	< Remove	

OK Cancel Apply

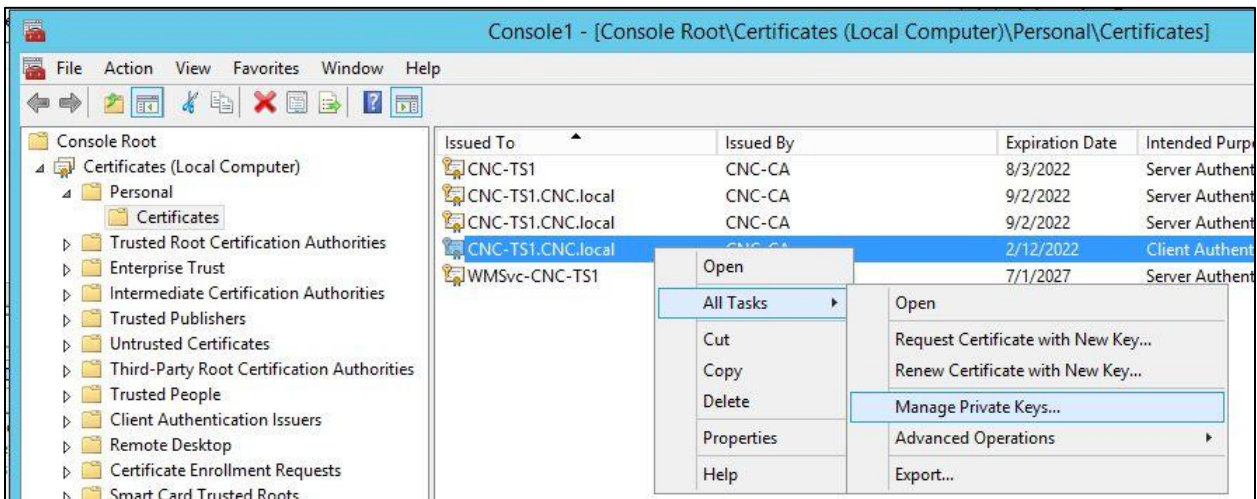


4.2.4 Generate SQL Certificate Request

Follow the same steps in the above section, to request a new certificate:

1. Select **Computer** for the template instead of "Web Server" from the previous two requests.
2. Select **Details** and then the **Properties** button.
3. Under the **General** tab enter a friendly name so this certificate can be easily identified later within SQL Server.
4. Select **OK** to close the **Certificate Properties** window.
5. Select the **Enroll** button from the main Certificate Enrollment window.
6. The certificate will now be available within the list of Personal certificates.
7. Locate the SQL certificate you just created by looking at the friendly name issued for the certificate. Right-click on the certificate and then select All Tasks>**Manage Private Keys...**

August 1, 2021



8. Add the account the SQL Server service is running under and give the account **Read** access. To locate the account SQL server is running under, open Server Configuration Manager>SQL Server Services and look in the Log On As column next to the correct SQL server instance. Select **OK**.

4.2.5 CA Root Certificate

The CA Root certificate should automatically import into the Trusted Root Certification Authorities for all computers on the domain. This may take up to 8 hours before available. If the CA Root is still not present on a machine, try to reboot the machine. If after reboot, the CA Root is still not available, then it can be manually imported into the Trusted Root Certification Authorities for that machine.

5 Install DoD root certificates with InstallRoot (Web Server)

Skip this section for password only setup.

MELD requires DoD root certificates for CAC for authentication. The DoD root certificates will need to be installed for MELD to properly authenticate.

Follow the steps within this article to **Install DoD root certificates with InstallRoot**.

<https://public.cyber.mil/pki-pke/end-users/getting-started/#toggle-id-1>

Important: Every client machine that is accessing MELD will need to perform this install as well.

5.1 Verify InstallRoot installed successfully

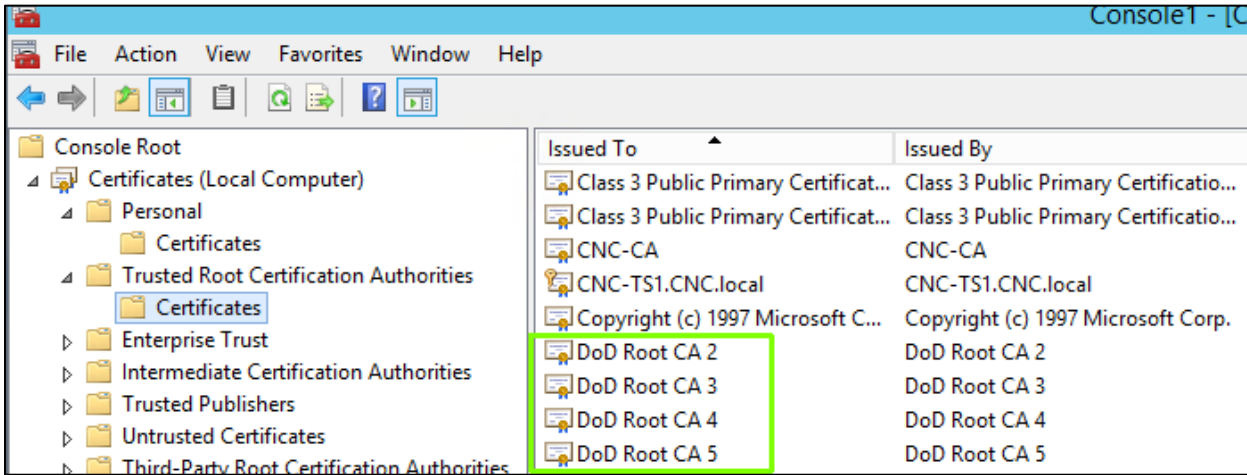
To verify the InstallRoot was successful:

1. Run the Microsoft Management Console by entering MMC in the search bar and then launching it.
2. Select File>Add/Remove Snap in...
3. Select Certificates in the left column and then select the Add button.
4. Select Computer Account.
5. Select Local Computer.
6. Select Finish and then select OK.
7. The Certificates snap in should now be loaded.

August 1, 2021

8. Select the Certificates folder location within Trusted Root Certification Authorities and ensure the DoD Root CAs are shown.

Note: The console window can be saved with the certificate Snap in to skip the above steps when accessing at a later time.



6 Setup Windows Roles and Features on the Web Server

August 1, 2021

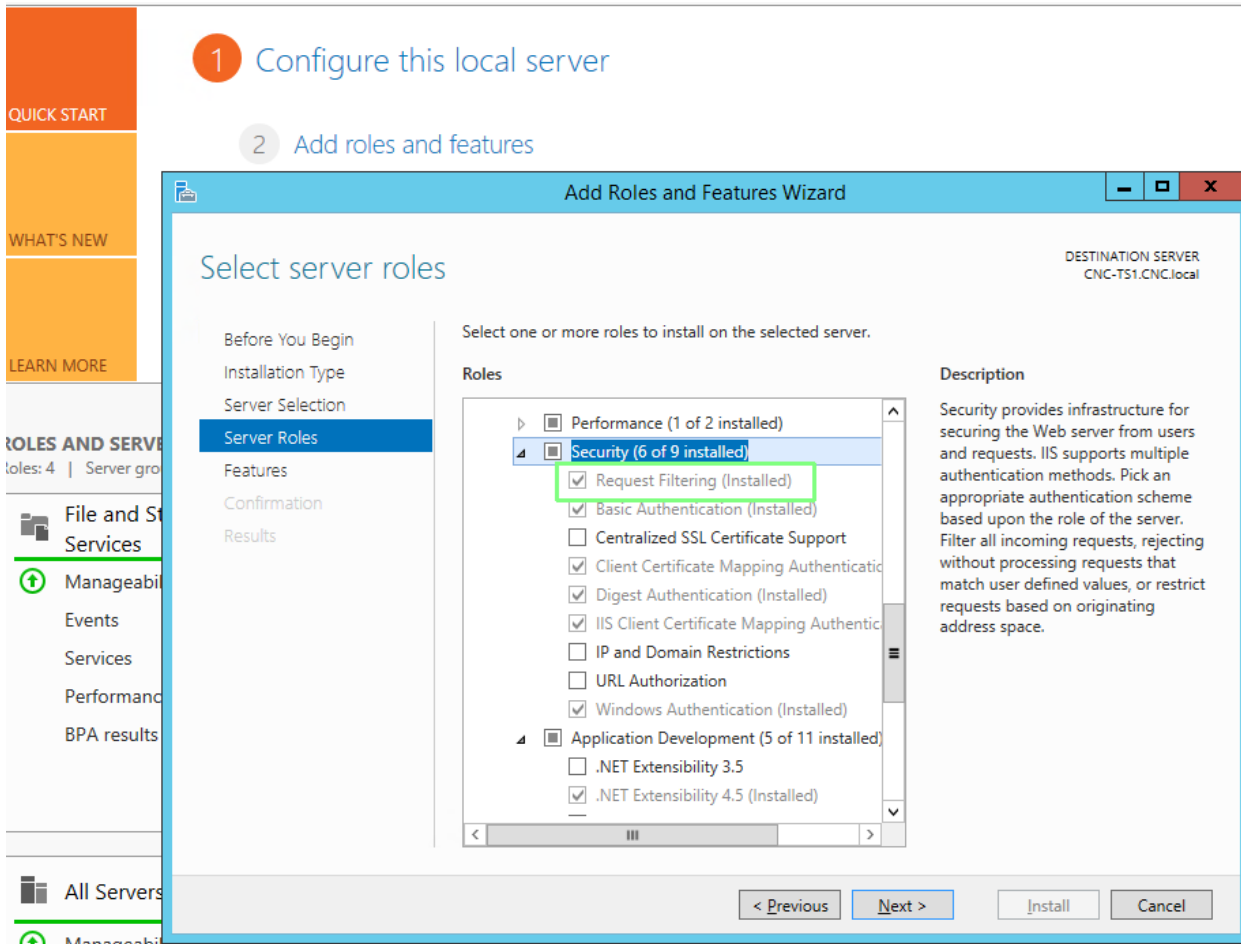
1. Click Start, point to **Administrative Tools**, and then click **Server Manager**.
2. On the Dashboard within the **Configure this local server** section select **Add roles and features**.
3. Keep default selection **Role-based or feature based installation** and select **Next**.
4. Ensure the web server is the one selected in the server pool listing and select **Next**.
5. Select the Web Server (IIS) role and ensure the following role services are selected:

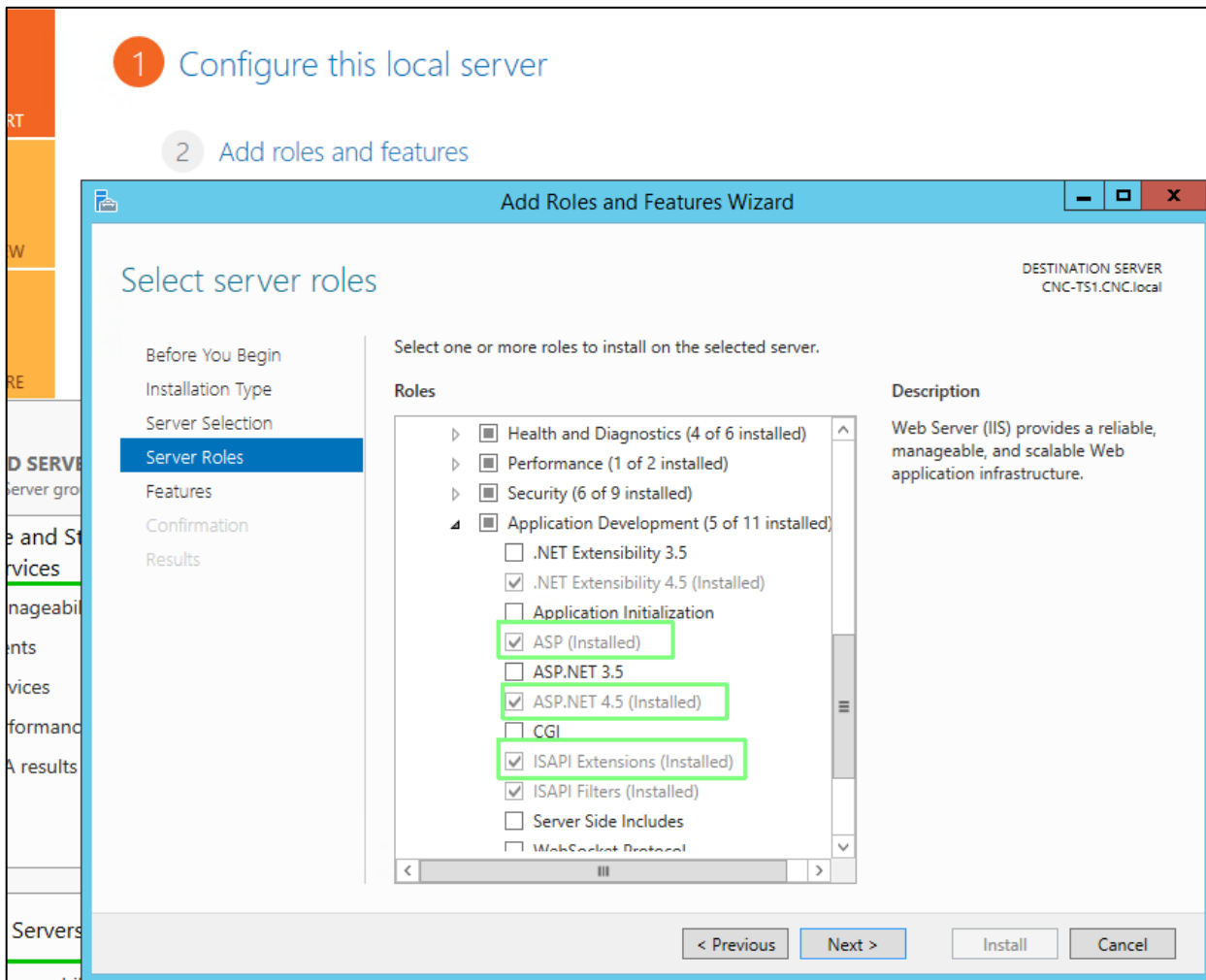
Shown in the first image:

- Request Filtering (within Security)

Shown in the second image (within Application Development):

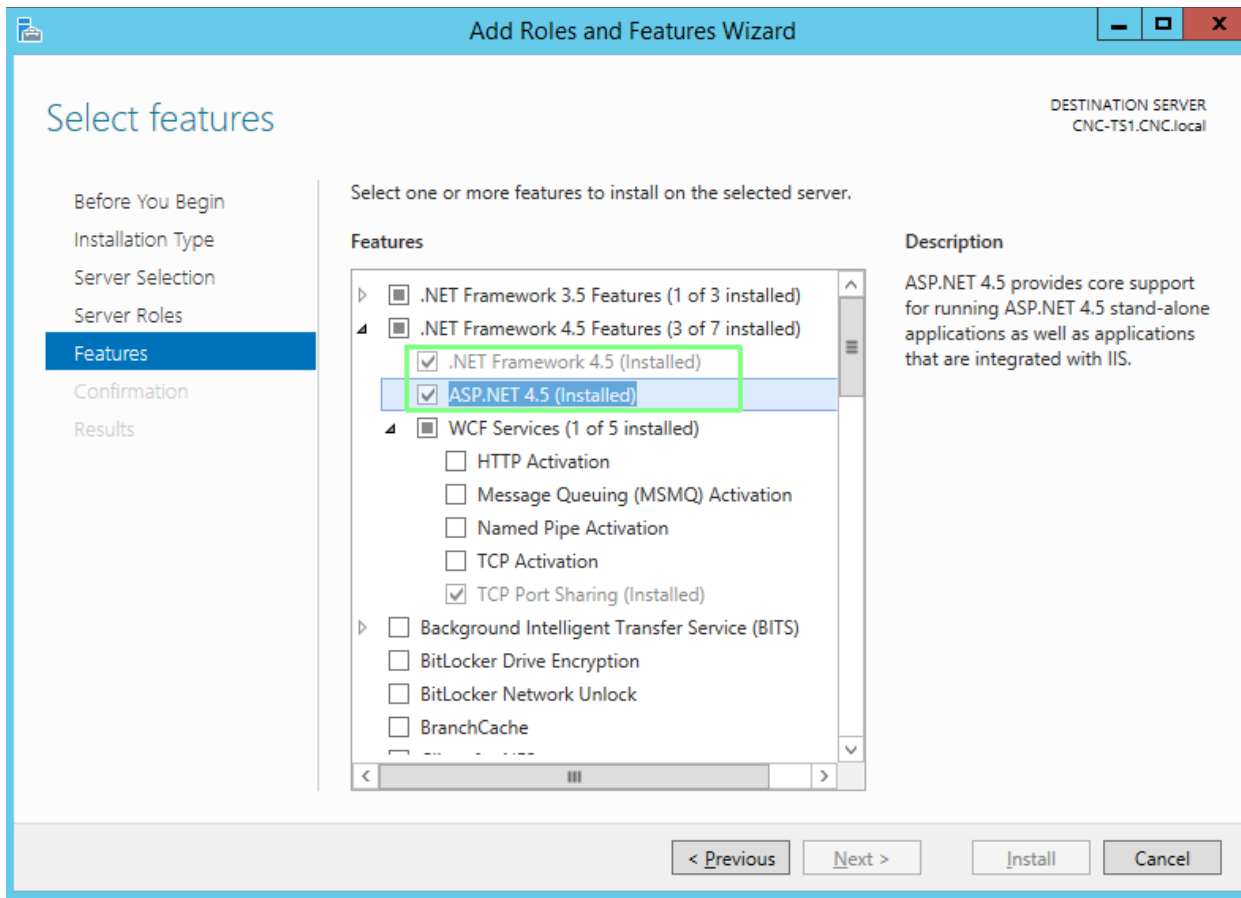
- ASP.NET 4.5 or later if listed
- ASP
- ISAPI Extensions





6. Select Next and ensure the following features are selected:

- .NET Framework 4.5 or later if listed
- ASP.NET 4.5 or later if listed



7. Select **Next** to continue and **Install**.

7 .NET Framework 4.8 (Web Server)

The .NET Framework 4.8 is required to run the .NET applications within MELD. If the server did not come with the 4.8 installation, then it will need to be downloaded and installed from Microsoft.

8 File System (Web Server)

8.1 Folder Copies

8.1.1 MELD Directory

Locate the MELD directory within this setup folder and copy to the wwwroot folder. This is typically located here: C:\inetpub\wwwroot.

8.1.2 IME_Data

Locate the IME_Data folder within this setup folder and copy to a location **outside** of the wwwroot folder. This folder will contain all the courseware files and can get very large. It is recommended to place this folder on another local hard drive that the windows operating system does not reside on, such as D or E. A sample location would be E:\IME_Data.

8.2 Folder Permissions

8.2.1 Inetpub

The inetpub folder contains application configuration files and is a DoD requirement to ensure that only administrators and necessary system accounts are the only accounts with permission to **alter** files within this folder.

Verify the permissions exist for the following users. Remove any additional permissions present. If any permissions have been removed simply make the change to this folder alone, **don't** select to replace all child object permissions. This would replace the default permissions created by IIS.

System: Full control
Administrators: Full control
TrustedInstaller: Full control
ALL APPLICATION PACKAGES (built-in security group): Read and execute
Users: Read and execute, list folder contents
Creator/Owner: Special permissions to subkeys

8.2.2 MELD/IME/Web.config

To prevent reading sensitive information that could be used to gain access to the database, there is a DoD requirement to only allow administrators and system accounts **read** access to the MELD /IME/Web.config .

Verify the permissions exist for the following users. Remove any additional permissions present.

System: Full control
Administrators: Full control
TrustedInstaller: Full control
ALL APPLICATION PACKAGES (built-in security group): Read and execute
Internet Guest Account: IUSR: Read and execute
IIS_IUSRS: YourComputerName\IIS_IUSRS: Read and execute
Creator/Owner: Special permissions to subkeys

8.2.3 MELD/global.asa

To prevent reading sensitive information that could be used to gain access to the database , there is a DoD requirement to only allow administrators and system accounts **read** access to the MELD/global.asa file.

Verify the permissions exist for the following users. Remove any additional permissions present.

System: Full control
Administrators: Full control

August 1, 2021

TrustedInstaller: Full control

ALL APPLICATION PACKAGES (built-in security group): Read and execute

“Internet Guest Account: IUSR”: Read and execute

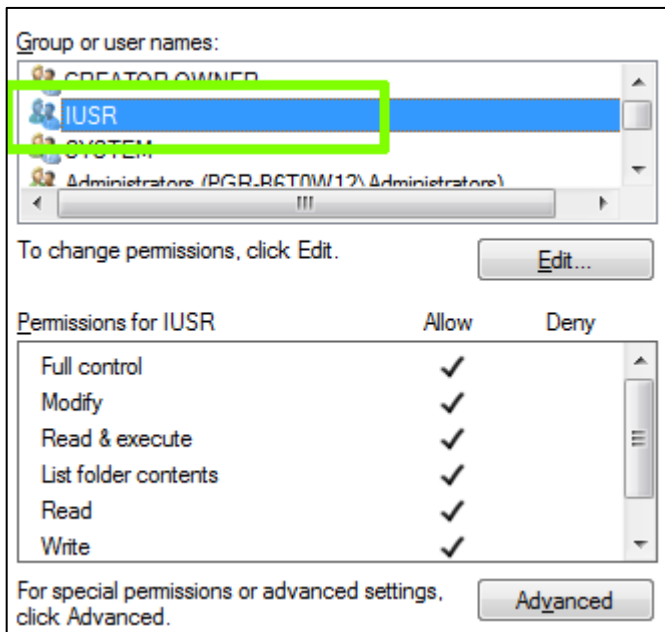
Creator/Owner: Special permissions to subkeys

8.2.4 Additional Folder Permissions

To enable project management the following permissions must be given to support the upload and creation of files. These folders can be safely modified by the following accounts, because these are not configuration files and do not contain sensitive information.

The following “Internet Guest Account: IUSR”, must be given modify, read, and write access to:

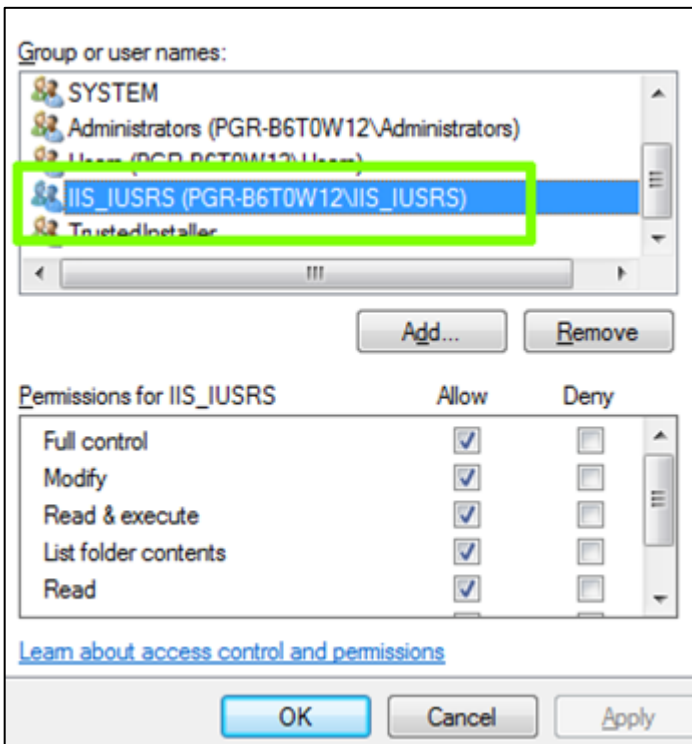
1. MELD\Projects
2. IME_Data (Note: This is the directory that is located outside of the wwwroot folder)
3. MELD\IME\Dictionary



The following IIS_IUSRS: YourComputerName\IIS_IUSRS must be given modify, read, and write access to:

1. IME_Data (Note: This is the directory that is located outside of the wwwroot folder)
2. MELD\IME\Dictionary

August 1, 2021



8.2.4.1 Log File and Tool Protection

In addition to the IUSR and IIS_IUSRS permissions above, the Authenticated_Users permission can be granted modify, read, and write access to the IME_Data folders, except the following two folders:

IME_Data\Log_Browser
IME_Data\IME_Logs

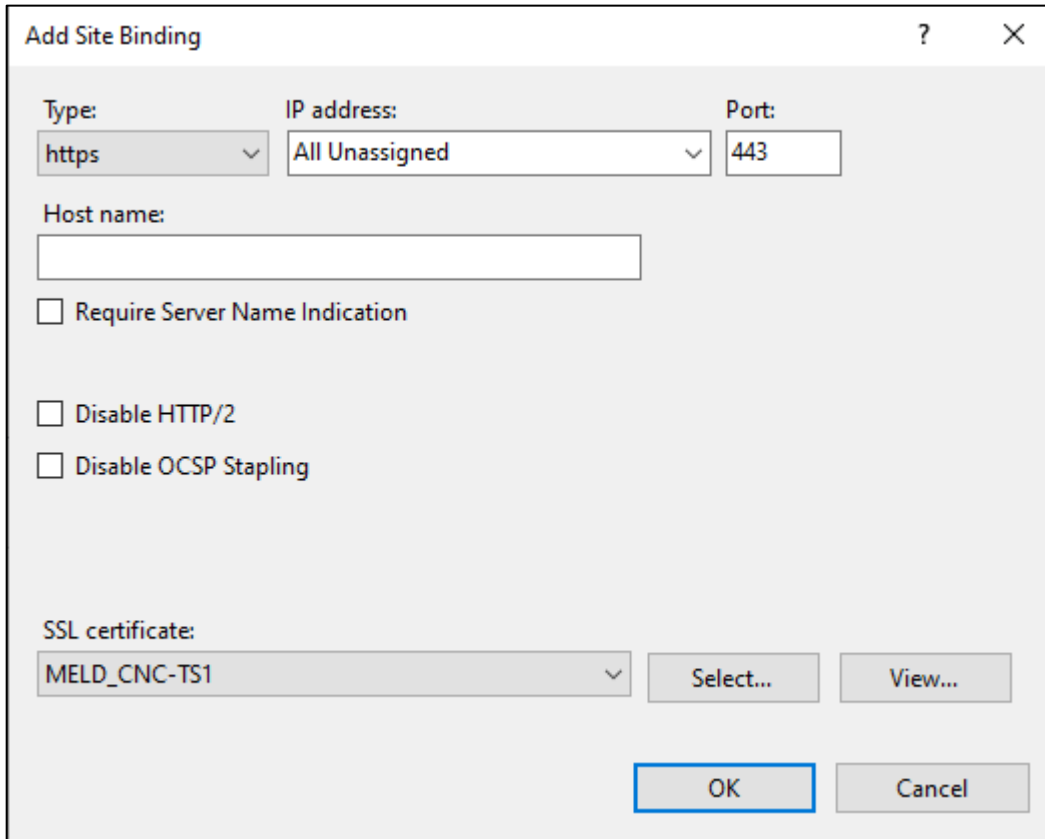
In addition to the system, IUSR, and IUSRS permissions, only system administrators should have access to these folders. This is a DoD requirement to protect the audit tools and logs from unnecessary access and modification.

9 Configure MELD website for SSL

9.1 Edit Binding

Open IIS and expand the Sites list. Right click on the web site MELD will be using and select **Edit Bindings...**

1. Add a binding to port **443** if it does not already exist. Select the Edit button if the binding already exists. *Note: 443 is the DoD approved port for https.*
2. Leave the IP address as **"All Unassigned"** or you can also enter a specific IP address for the web server.
3. If the website will be using a host name, such as "MELD", enter the **Host name**. If no host name is entered the computer name or IP can be used within the URL to access the site. *Note: This host name must be added as a DNS entry, and also listed as an Alternate name / DNS on the web server certificate.*
4. Select the web site certificate that was obtained by the DoD or that the project created from the Certificate Authority.



Add Site Binding

Type: **https** IP address: **All Unassigned** Port: **443**

Host name:

Require Server Name Indication

Disable HTTP/2

Disable OCSP Stapling

SSL certificate: **MELD_CNC-TS1** **Select...** **View...**

OK **Cancel**

9.2 Enable Client Certificate Negotiation

Skip this section for password only setup.

The **Enable Client Certificate Negotiation** setting is required for working with client certificates.

The **Disable Client Certificate Revocation Check** is recommended during this initial setup to allow CAC authentication on standalone systems. The standalone systems will not be able to load the certificate revocation list on the DISA site and may fail authentication if a local certificate revocation list cache is not available. This will initially not be available, which is recommend to disable the client certificate revocation check initially.

Follow the steps below to alter these settings:

Open the command prompt *as an administrator* and enter the below text to get values for <app id> and <cert hash>. There may be multiple entries returned. Look for the entry with the 443 port.

```
netsh http show sslcert
```

Select the text within the command window and copy and paste into NotePad.

Run the command window again with the <cert hash> and <app id> replaced with the actual values. If the ip address is included with the port, then replace the 0.0.0.0 with the ip address.

```
netsh http delete sslcert 0.0.0.0:443  
netsh http add sslcert 0.0.0.0:443 <cert_hash> {<app_id>} clientcertnegotiation=enable verifyclientcertrevocation=disable
```

August 1, 2021

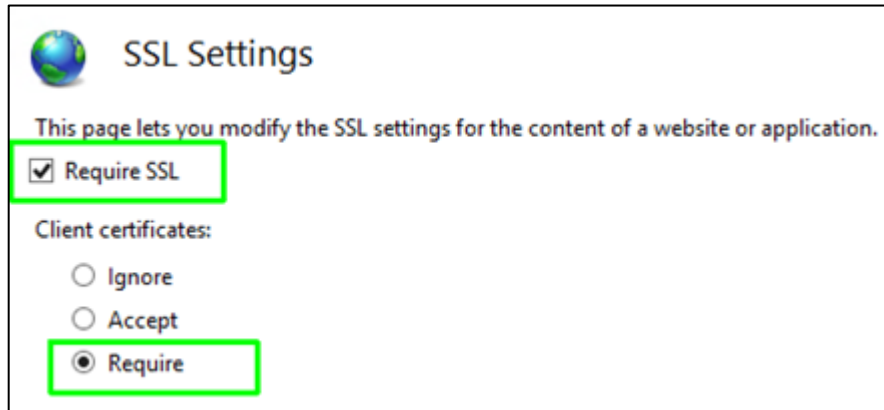
Finally, run the `netsh http show sslcert` command again to verify that **Negotiate Client Certificate** is showing **Enabled** and **Verify Client Certificate Revocation** is showing **Disabled**. Make sure to reference the listing with the 443 port and your matching IP (if included with the port).

```
SSL Certificate bindings:
-----
IP:port                : 0.0.0.0:443
Certificate Hash       : bf7b3055bd1118ebabeb97faf6d6ccb560f7a4f6
Application ID        : <4dc3e181-e14b-4a21-b022-59fc669b0914>
Certificate Store Name : <null>
Verify Client Certificate Revocation : Disabled
Verify Revocation Using Cached Client Certificate Only : Disabled
Usage Check           : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout : 0
Ctl Identifier        : <null>
Ctl Store Name       : <null>
DC Mapper Usage      : Disabled
Negotiate Client Certificate : Enabled
```

9.3 Require SSL and Client Certificates

Within IIS, select the website MELD will be using and then select **SSL Settings**.

1. Select **Require SSL**
2. Select **Require Client Certificates**
Skip this selection for password only setup.

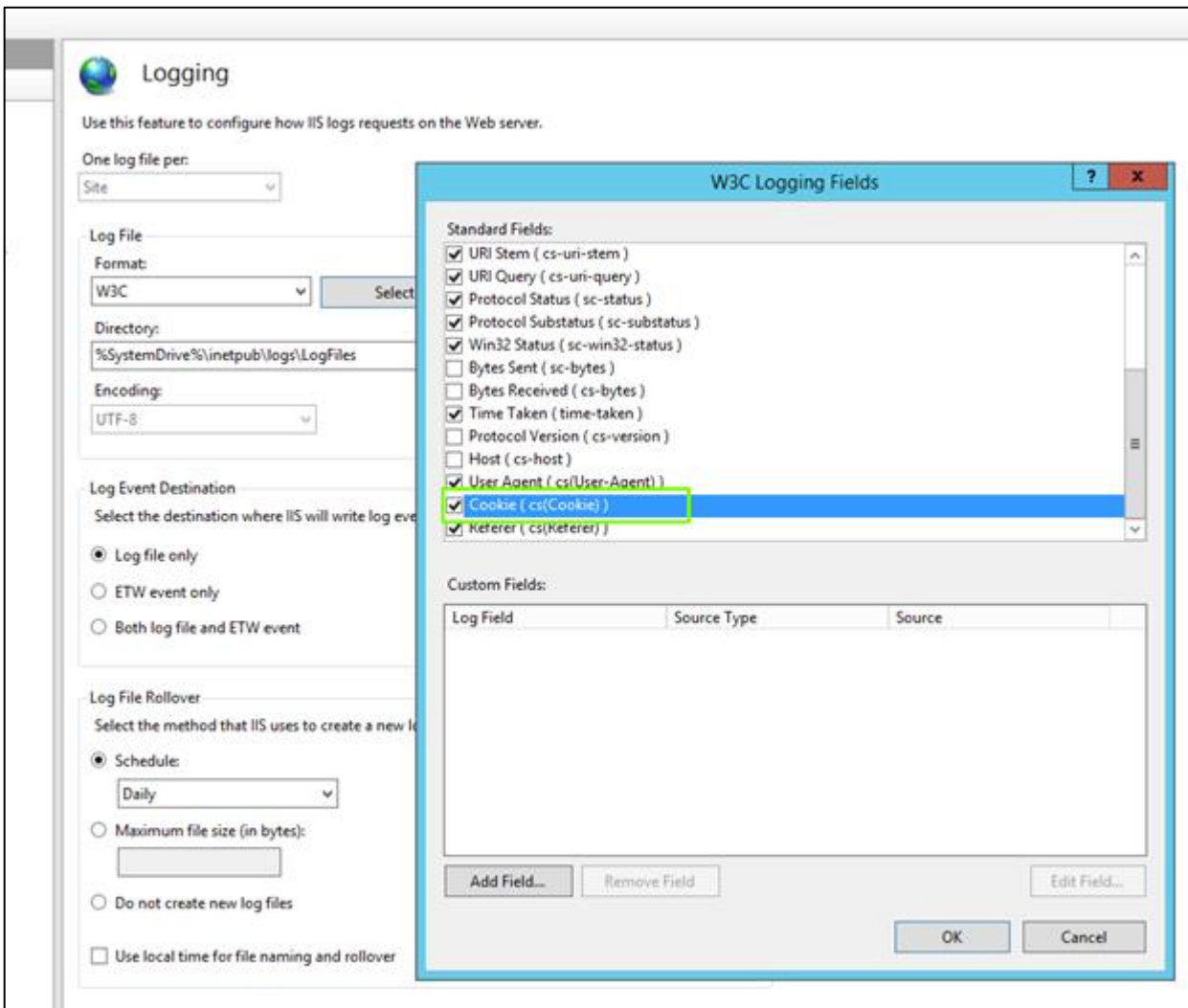


3. Select **Apply** under Actions to save changes.

9.4 Update Logging

The DoD requires error logging to include the ASP.NET session id. This value is also very helpful for further investigation from the MELD generated logs. With both logs producing the ASP.NET session id this value can be used to identify exactly when a certain user was on the system and the full user activity. Follow the below steps to include the session id with the IIS logs.

1. Within IIS, select the website MELD will be using and then select **Logging**.
2. Select the **Select Fields** button.
3. Check the **Cookie** checkbox.
4. Select the **OK** button.
5. Select the **Apply** to save changes.



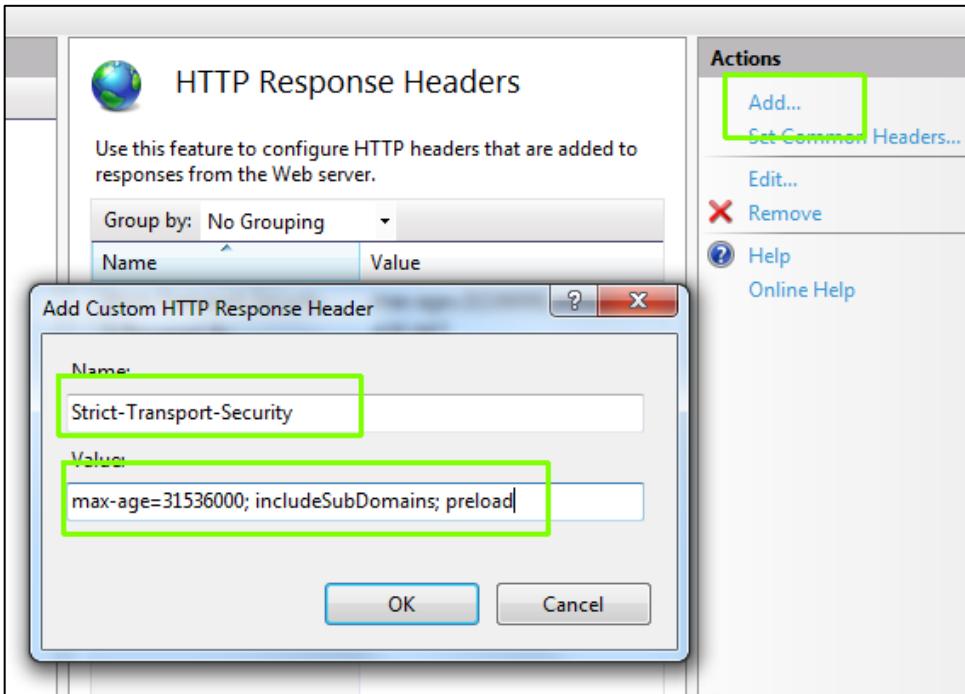
10 Enable HSTS on MELD website

The DoD requires that HSTS is enabled for the website. The HSTS lets a web site tell browsers that it should only be accessed using HTTPS, instead of using HTTP.

To enable HSTS:

1. Within IIS, select the website MELD will be using and then select **HTTP Response Headers**.
2. Click **Add** in the actions section.
3. A new form will appear "Add Custom HTTP Response Header".
4. Enter **Strict-Transport-Security** for the **Name** field.
5. Enter **max-age=31536000; includeSubDomains; preload** for the **Value** field.

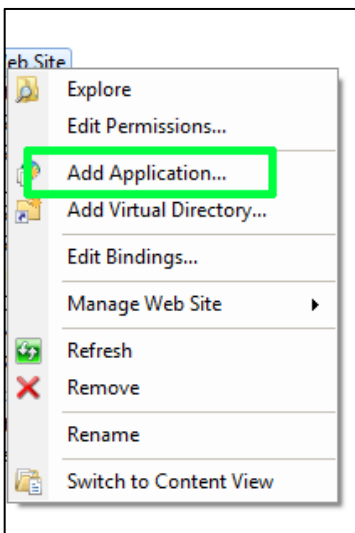
August 1, 2021



6. Select **OK**.
7. The HSTS header will now be added within the Response Headers listing.

11 Create MELD Application (IIS)

To create the MELD application open IIS and expand the Sites list. Right click on the web site MELD will be using and select **Add Application...**

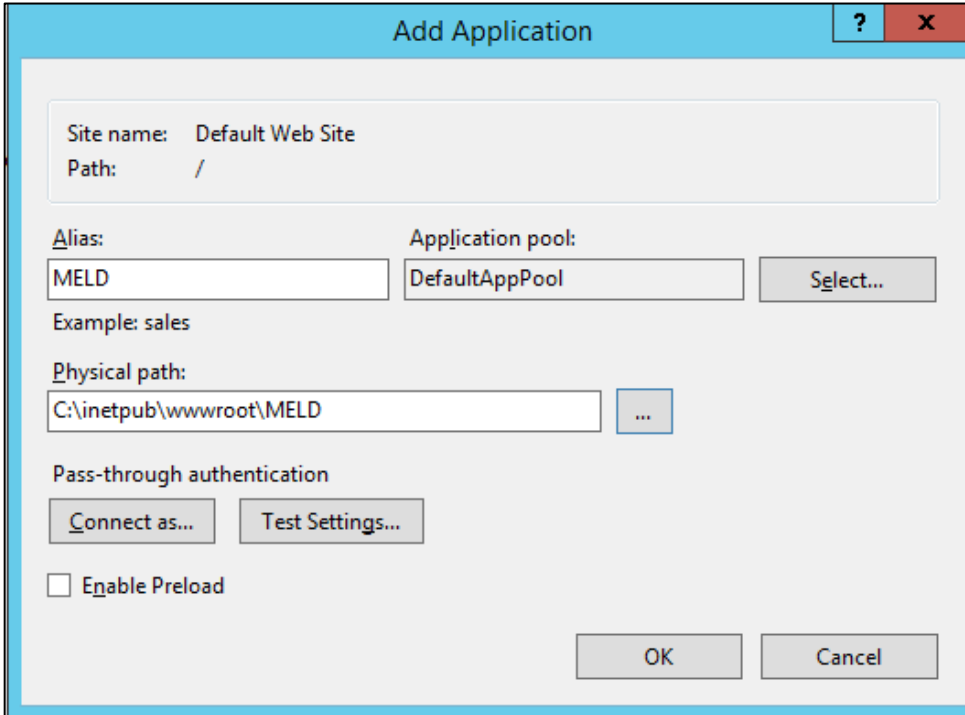


An Add Application form will appear.

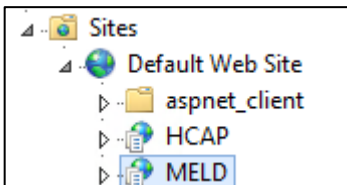
- Type **MELD** in the Alias field.

August 1, 2021

- Note the Application pool. By default the application pool will be attached as the “DefaultAppPool”. A new application pool can be created and changed if desired.
- Browse for the MELD folder that was copied to the web server, typically copied to the “wwwroot” folder.
- Select OK.

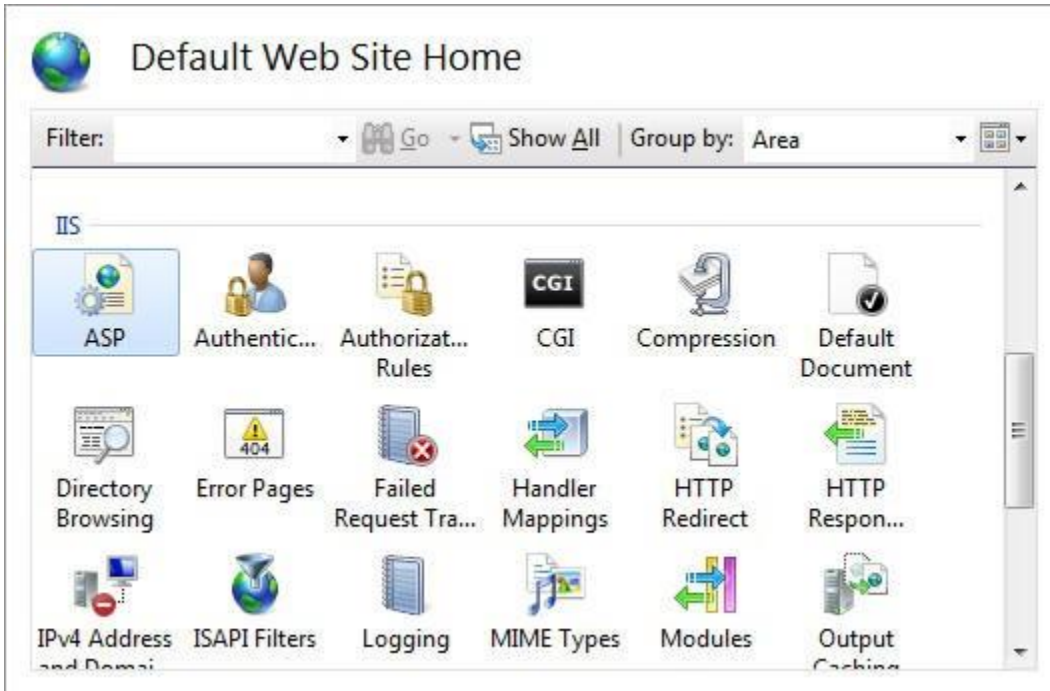


The application will now appear in the web site listing:

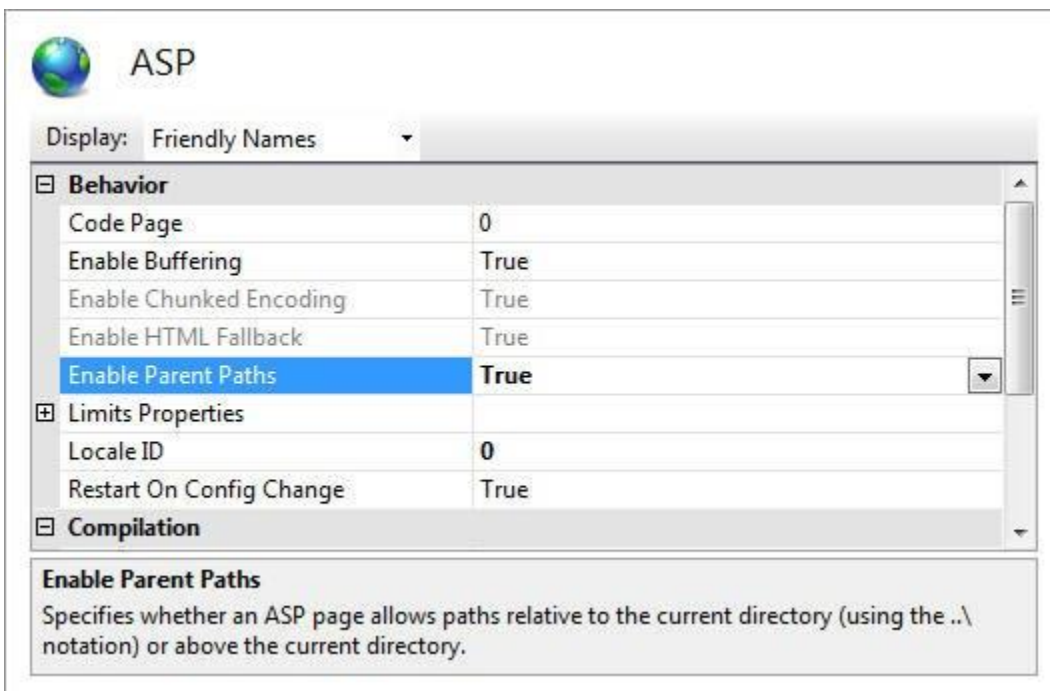


11.1 Enable Parent Paths (IIS)

The MELD application needs parent paths to be enabled. To do so, open IIS Manager and navigate to the MELD application, and then-double click the ASP feature.

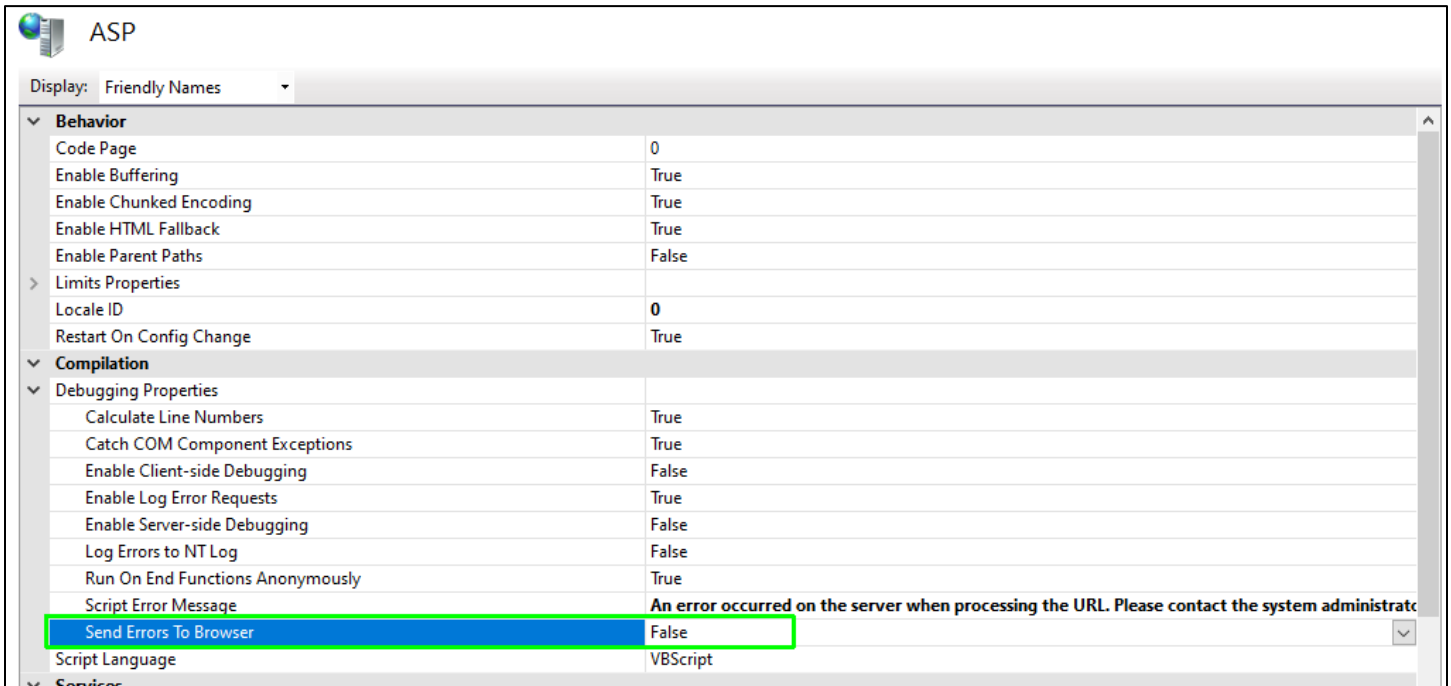


In the list of ASP features, enable the **Enable Parent Paths** option by selecting **True**. Select **Apply** to save the changes.



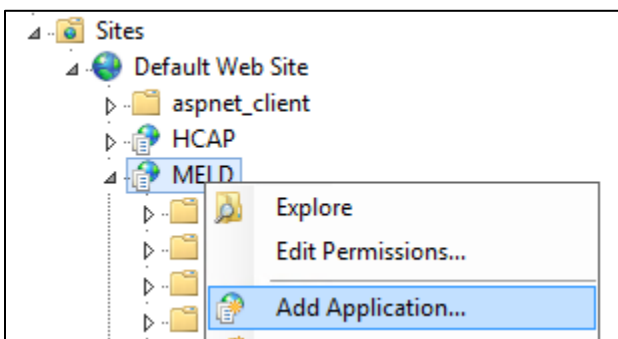
11.2 Error Browser Settings

A DoD requirement is to not allow script errors to appear within the browser window. To ensure these errors do not display to the user, check that the setting **Send Errors To Browser** within Debugging Properties is set to **False**. Select **Apply** to save any changes.



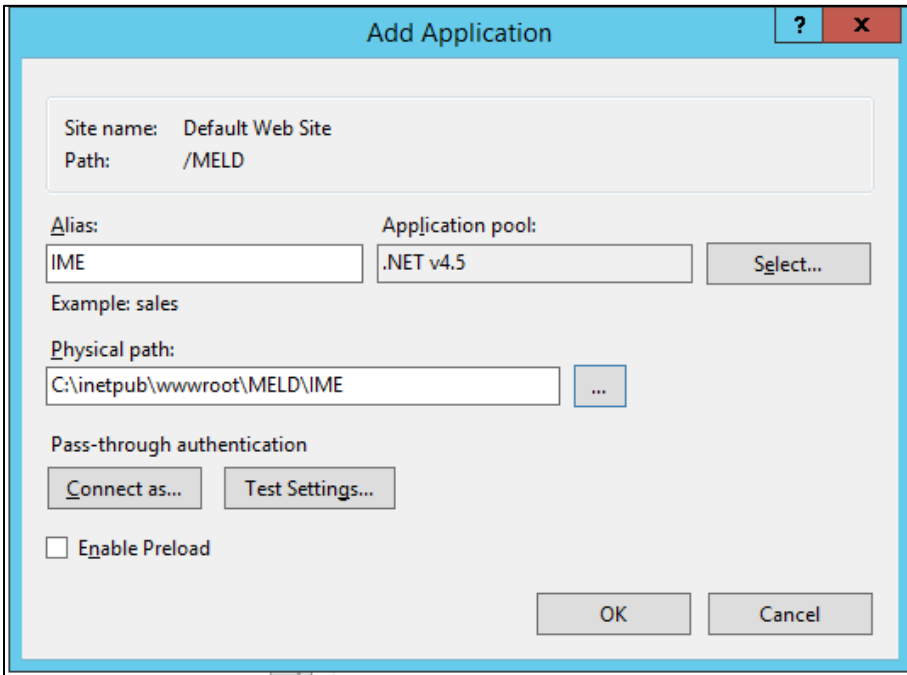
11.3 Create IME Application (IIS)

To create the IME application, locate the MELD application within IIS. Right click on the MELD application and select "Add Application".



An Add Application form will appear.

- Type **IME** in the Alias field.
- Switch the Application pool to **.NET v4.5**
- Browse for the IME folder located within the MELD folder that was copied to the web server, typically copied to the "wwwroot" folder.
- Select **OK**.



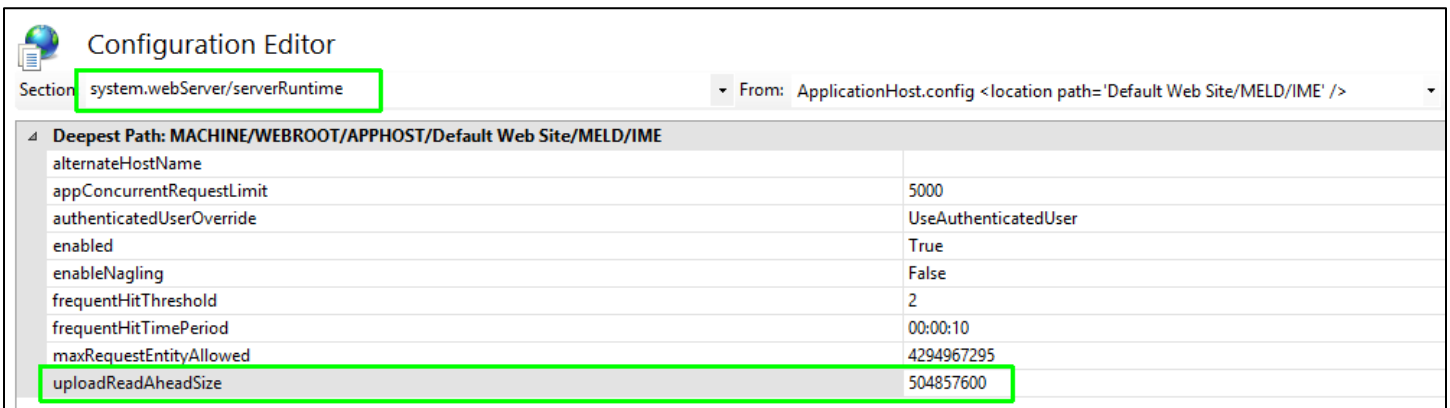
The application will now appear in the web site listing.

11.3.1 Setup uploadReadAheadSize

SSL requires the read ahead size to be set to your upload limit size (500MB) to prevent data retrieval errors.

Follow the below steps to increase the read ahead size to 500MB:

1. Select the IME application within IIS and then select **Configuration Editor**
2. Select **system.webServer/serverRuntime** from the drop down menu
3. Look for the **uploadReadAheadSize** and change the value to **504857600**.
4. Select the **Apply** button to save the changes.

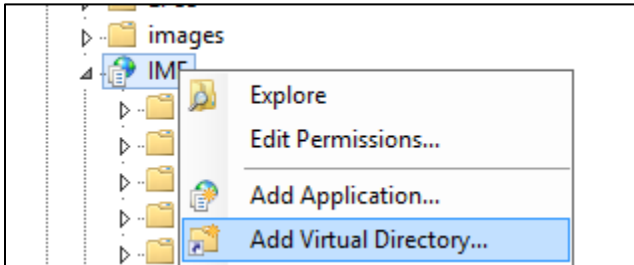


11.3.2 Create IME Data Virtual Directories (IIS)

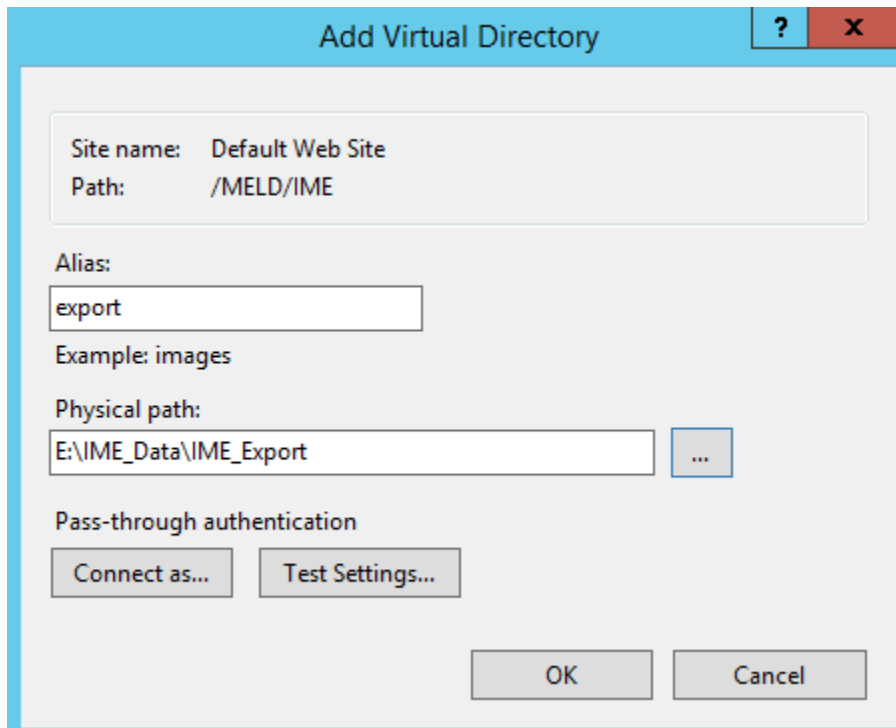
The IME_Data folder located outside of the wwwroot location stores the files used to create the courseware exports, the courseware exports, and all temporary files used for imports and previewing courseware. These folders are accessible to the MELD application by using virtual directories.

11.3.2.1 Create Export Virtual Directory (IIS)

Right click on the IME application and select **Add Virtual Directory...**



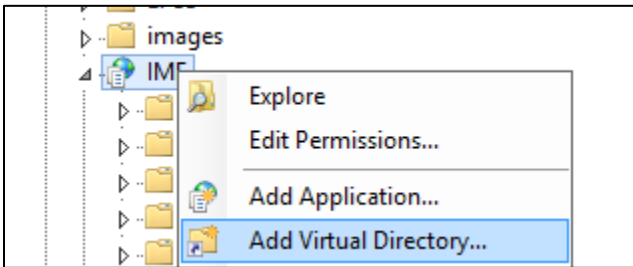
1. Enter **export** for the Alias.
2. Browse for the IME_Export folder within the IME_Data location.
3. Click **OK**



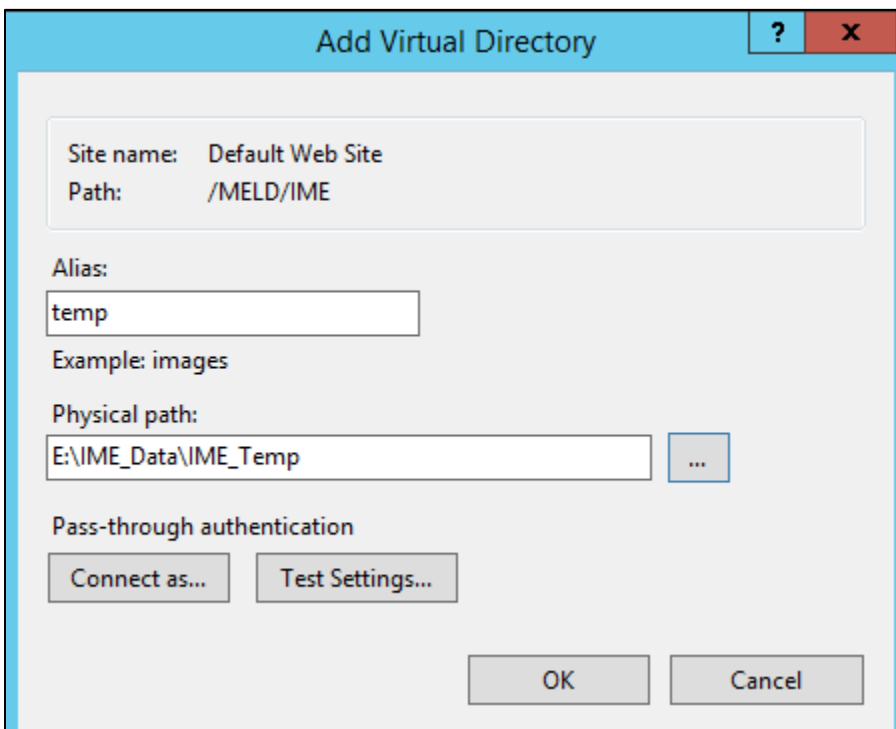
11.3.2.2 Create Temp Virtual Directory (IIS)

Right click on the **IME** application and select **Add Virtual Directory...**

August 1, 2021



1. Enter **temp** for the Alias.
2. Browse for the IME_Temp folder within the IME_Data location.
3. Click **OK**

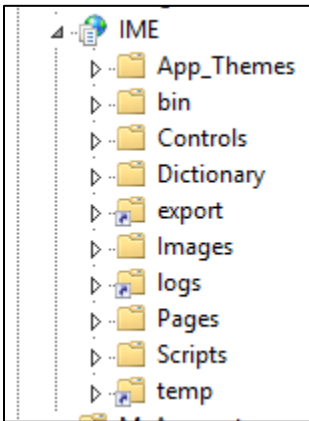


11.3.2.3 Create Logs Virtual Directory (IIS)

Right click on the **IME** application and select **Add Virtual Directory...**

1. Enter **logs** for the Alias.
2. Browse for the IME_Logs folder within the IME_Data location.
3. Click **OK**

The IME application within IIS should now look like this:



11.4 Application pool settings

11.4.1 Update application pool recycling options

The application pool recycling options will recycle every 1740 minutes. This will log all users out of MELD every 1740 minutes. This is not ideal and should be updated to recycle during off hours.

To change the recycling options follow the below steps:

1. Within IIS, select the application pool(s) used for the MELD application.
2. Select **Recycling**.
3. Uncheck **Fixed Intervals**.
4. Select the **Specific times(s)** checkbox and enter a specific time frame when users would not typically be on the server.
5. Select **Next** and then finish to complete the change.

The screenshot shows the 'Edit Application Pool Recycling Settings' dialog box. The 'Recycling Conditions' section is highlighted with a green box. It contains the following options:

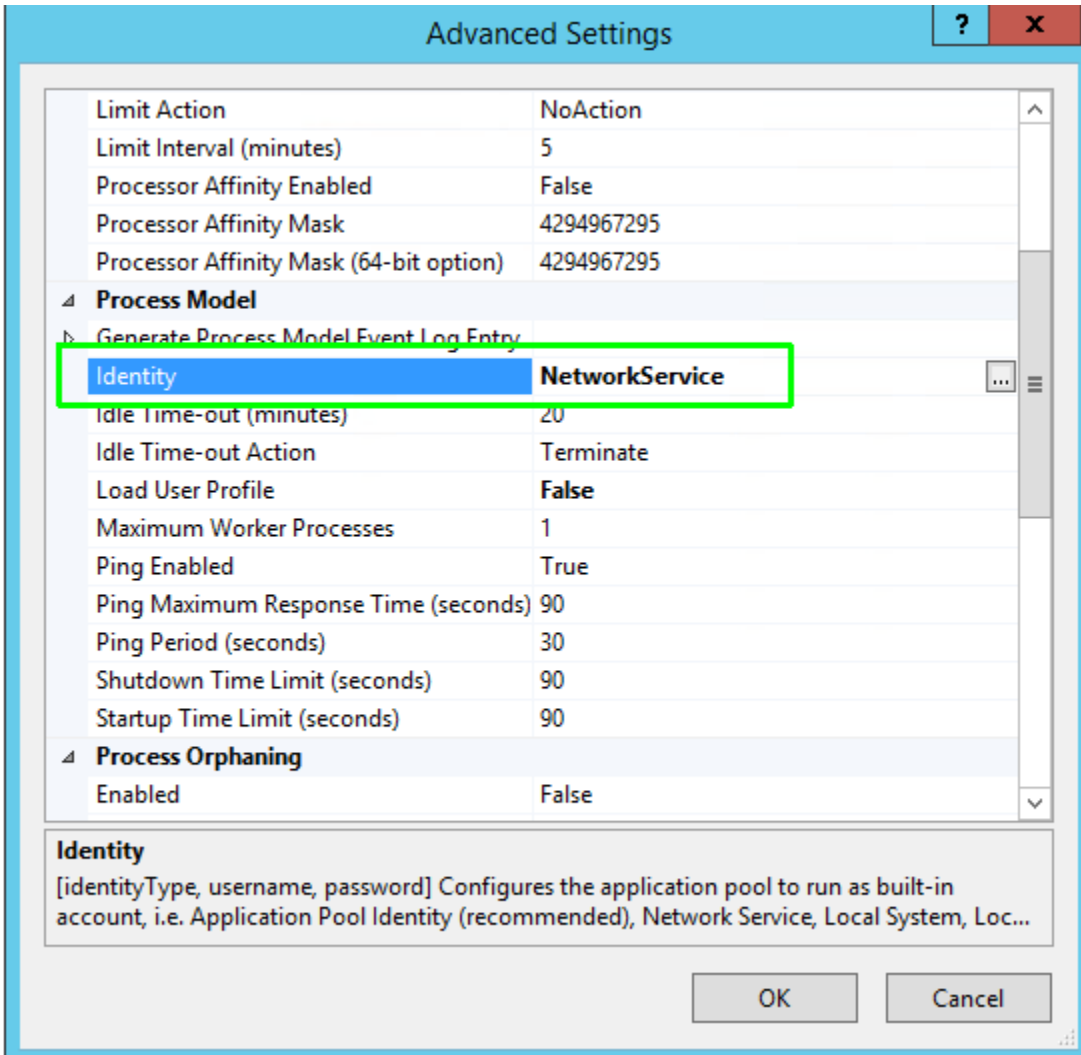
- Regular time intervals (in minutes):
- Fixed number of requests:
- Specific time(s):
 - Text box: 12:00 AM
 - Example: 8:00 PM, 12:00 AM
- Virtual memory usage (in KB):
- Private memory usage (in KB):

Navigation buttons: Previous, Next, Finish, Cancel.

11.4.2 Update application pool identity

The application pool(s) needs to set the Identity to **NetworkService** to support the SMTP service and the audit log reporting services.

Within IIS, locate the application pool used by MELD and IME and select **Advanced Settings** to change the Identity. Select **NetworkService** from the drop down menu.



11.4.3 Increase Session Timeout (IIS)

The DoD requires a timeout after 15 minutes for a standard user and 10 minutes for a user with elevated permissions. However, if an exception is made for this timeout value, then it can be changed below to satisfy the site requirement.

The default timeout for an application within IIS is set to timeout after 20 minutes. If the user has not actively submitted data within the time period the application will timeout and the user will need to enter their credentials to access MELD again. To increase this timeout, locate each application pool used within MELD. This is typically the default application pool and the .NET 4.5 application pool, unless changed when the applications were added within IIS.

1. Right click on each application pool and select "Advanced Settings"
2. Scroll until "Idle Time-out (minutes)" is located.
3. Increase the time-out to the desired time out period.
4. Close the Advanced Settings Window.

11.4.3.1 Increase Timeout in Configuration Files

If the timeout value is increased within the application pool, it will also need to be increased within the global.asa file. This is explained in more detailed within section **“Update Configuration Files within MELD (Filesystem)”**.

11.5 URL Rewrite

The URL Rewrite module is required to set the DoD requirement for the HTTPOnly attribute for the classic ASP session cookies used within IIS. This will prevent JavaScript access to these session cookies.

11.5.1 Install

To install the module, it will need to be downloaded from Microsoft here:

<https://www.iis.net/downloads/microsoft/url-rewrite>

Download the x64installer (all downloads appear as a listing at the end of the page).

11.6 MIME types

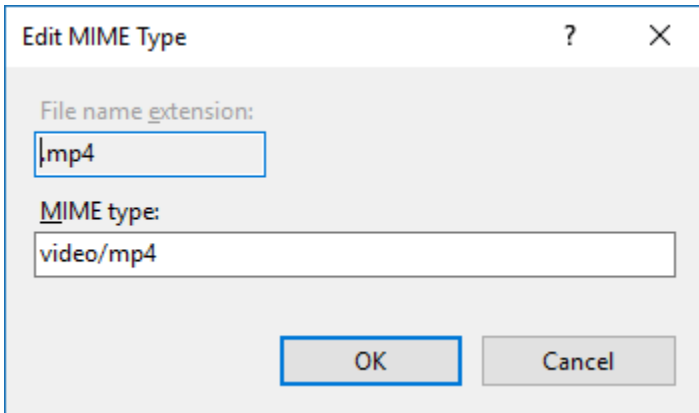
Lessons typically contain movie files, which will not display by default. The MIME types will need to be added to display movies within lessons.

Within IIS, select the server name and then select **MIME Types**. Select **Add...** to add a new MIME type.

The screenshot shows the IIS Manager interface for configuring MIME types. The main pane displays a table of existing MIME types. The 'Add...' button in the Actions pane is highlighted with a green box, indicating the next step in the process.

Extension	MIME Type	Entry Type
.323	text/h323	Local
.3g2	video/3gpp2	Local
.3gp	video/3gpp	Local
.3gp2	video/3gpp2	Local
.3gpp	video/3gpp	Local
.aac	audio/aac	Local
.aaf	application/octet-...	Local
.aca	application/octet-...	Local
.accdb	application/msac...	Local
.accde	application/msac...	Local
.accdt	application/msac...	Local
.acx	application/intern...	Local
.adt	audio/vnd.dlna.adts	Local
.adts	audio/vnd.dlna.adts	Local
.afm	application/octet-...	Local
.si	application/octe...	Local

The extensions **.mp4** and **.mp4v** should both be added and mapped to **video/mp4**.



12 SQL Server

SQL Server versions 2008 and above may be installed to run the MELD application.

Note: For a test environment SQL Server Express may be installed. For a live production site, the full version of SQL Server is recommended.

Important: It is a DoD requirement that SQL Server must be installed on a drive separate from the operating system drive.

12.1 Microsoft SQL Server Management Studio

Ensure SQL Server Management Studio is installed during the SQL Server installation. This enables an interface to attach the databases and add the user accounts explained in the next topic.

12.2 Server Authentication

Ensure the Server Authentication is set to **“SQL Server and Windows Authentication”** when installed. This establishes access to the MELD databases from the MELD applications. Individual users will login through the MELD application and not have access to the SQL server text based password, which makes this approach low risk. This level of risk is accepted by the ISSO/ISSM.

12.3 SQL Server Management Studio

12.3.1 Copy Databases

Copy the databases and database log files within the Databases folder located within this setup folder to the Microsoft SQL Server Data folder on the server.

Attach databases within SQL Server Management Studio from this location. The databases are titled:

- CoDE
- FEA

August 1, 2021

- CMATT
- COI
- TSSR
- Workflow

12.3.2 Create EXEC role

The db_executor role will need to be added to each database to support executing stored procedures. To add the role, copy and paste the text below and run within SQL Server Management Studio

Use CoDE

```
CREATE ROLE db_executor
```

```
GRANT EXECUTE TO db_executor
```

Use FEA

```
CREATE ROLE db_executor
```

```
GRANT EXECUTE TO db_executor
```

Use CMATT

```
CREATE ROLE db_executor
```

```
GRANT EXECUTE TO db_executor
```

Use COI

```
CREATE ROLE db_executor
```

```
GRANT EXECUTE TO db_executor
```

Use TSSR

```
CREATE ROLE db_executor
```

```
GRANT EXECUTE TO db_executor
```

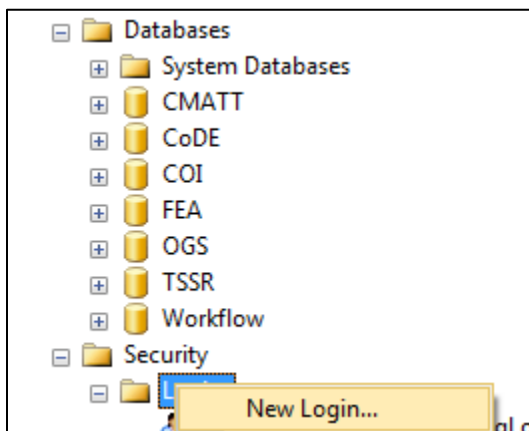
Use Workflow

```
CREATE ROLE db_executor
```

```
GRANT EXECUTE TO db_executor
```

12.3.3 Create MELD SQL Server Account

Select **Security>Logins>New Login...**



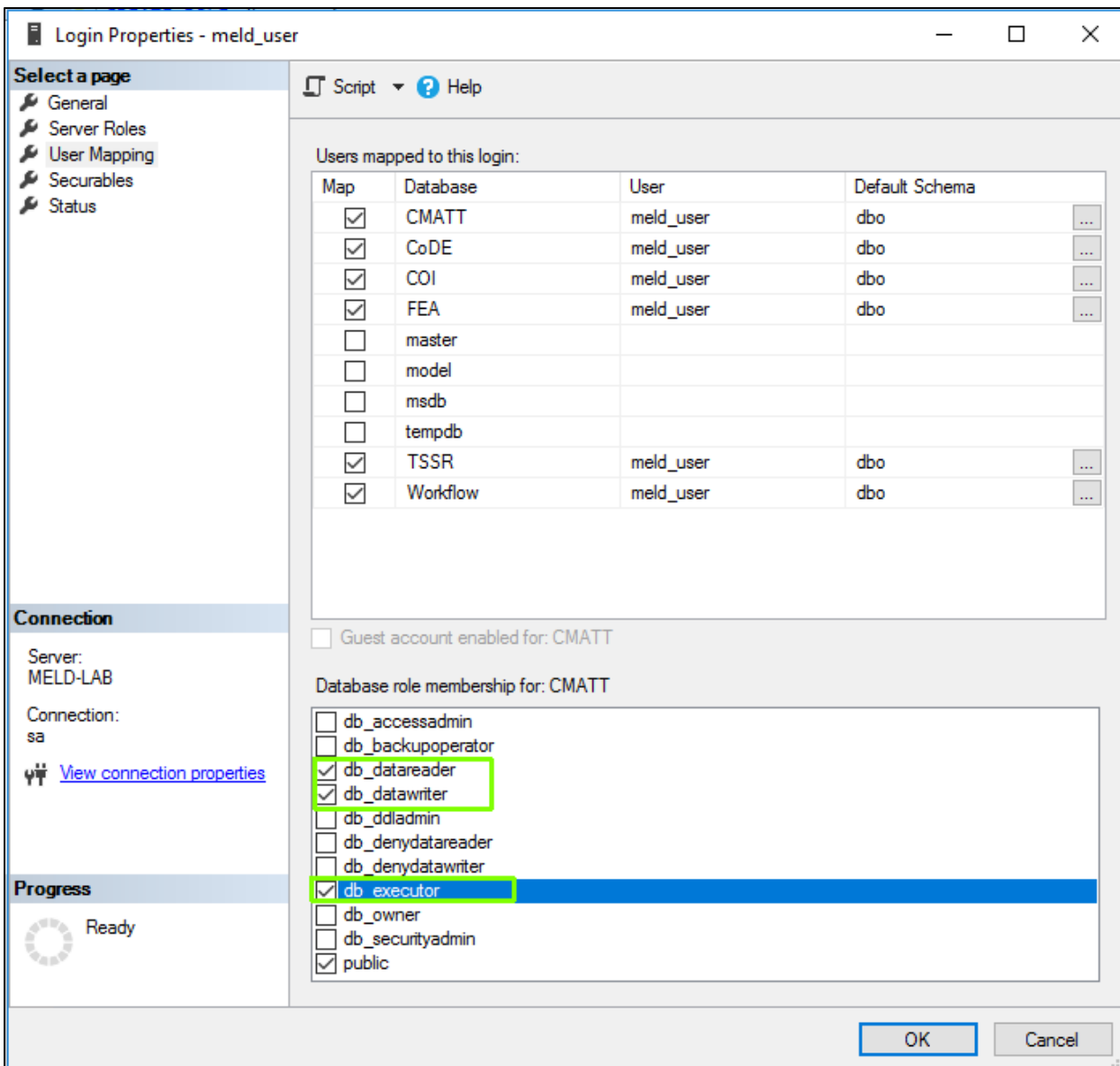
Enter the following information:

1. Login name: meld_user
2. Password: desired password
3. A DoD requirement on specific systems is to check: **Enforce password policy**
4. A DoD requirement on specific systems is to check: **Enforce password expiration**

Important: If you are on a specific system required by DoD to enforce password policy on SQL server accounts, then it is critical to be familiar with the policy set on your network and to set alerts to remind you BEFORE the password expires to update the password within SQL server AND the MELD configuration files. (section "Update Configuration Files within MELD (File System)".

Important: If enforce password policy is selected for the SQL account and password policy is set to require a user to change the password after first login, then MELD will fail when launching for the first time and a 500 Generic Server Error will appear on screen until the meld_user password is changed. After the password is changed the configuration files will need to be updated to reflect the new password (section "Update Configuration Files within MELD (File System)".

5. Select the User Mapping page / link within the same form.
6. Check each database and then check the **db_datareader** , **db_datawriter**, and **db_executor** role for each.



August 1, 2021

7. Double check each database and make sure the **db_datareader** and **db_datawriter**, and **db_executor** are assigned to each. With the number of databases this step could get overlooked and needs to be double checked before moving forward.
8. Select **OK**.

12.3.4 Set Password Dates

Run the following script to ensure the admin account does not get disabled due to expired dates within the database. To execute the script, copy and paste the text below and run within SQL Server Management Studio.

```
Use CODE
Update [user] set pwd_date = DATEADD(DAY, -70, GETDATE())
GO

UPDATE      [user]
SET         locked = 0, last_signed_on = GETDATE()
GO
```

12.3.5 Additional SQL Server Accounts

There should be no other additional SQL server accounts required to support the MELD application. If any other accounts are present, and are not used for other active applications, they should be removed.

Only authorized Windows Administrators should have access to the SQL server databases to support database maintenance. These administrators should use their Windows account to login to the SQL Server Management Studio and should not have individual SQL server accounts.

12.4 Install OLE DB Driver for SQL Server

To support TLS 1.2, a new driver will need to be installed. Follow the below link from Microsoft to install the OLE DB driver.

<https://docs.microsoft.com/en-us/sql/connect/oledb/applications/installing-oledb-driver-for-sql-server?view=sql-server-ver15>

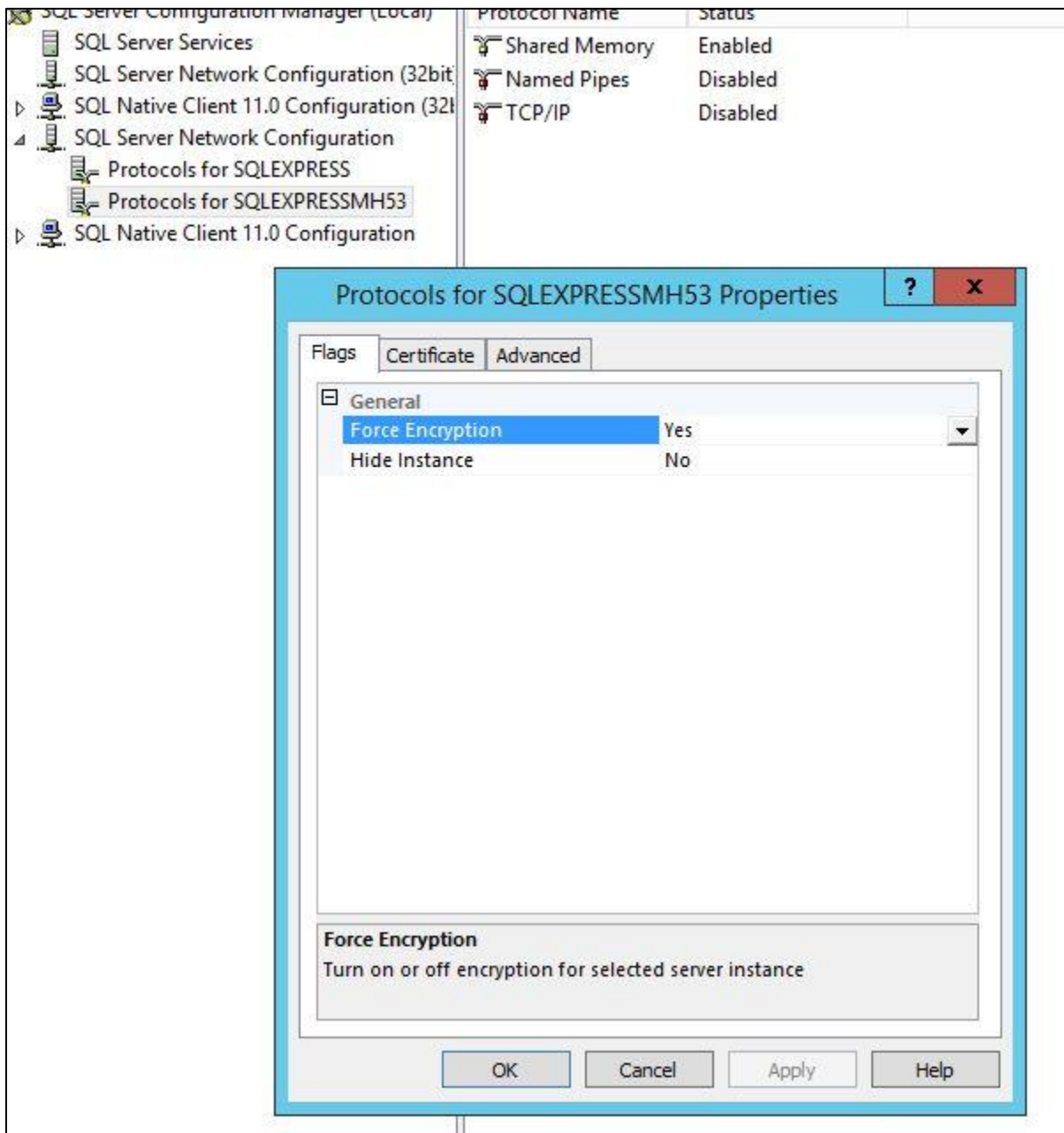
12.5 Update SQL encryption

Navigate to **SQL Server Configuration Manager > SQL Server Network Configuration**. Right-click on Protocols for the correct SQL instance, , and click on **Properties**.

Under the **Flags tab**, set **Force Encryption** to **Yes**.

Under the **Certificate** tab, select the SQL certificate created or obtained from the DoD within the “DoD SSL certificates section” of this document.

Select **OK** to complete the setup.



13 Update Configuration Files within MELD (File System)

13.1 Global.asa

Simply open the **global.asa** using NotePad within the wwwroot MELD folder to update the following settings. A typical path to the global.asa is located here C:\inetpub\wwwroot\MELD.

13.1.1 Connection Strings

The connection string read by MELD will need to be updated to reflect the SQL server name and MELD SQL server account.

August 1, 2021

The connection lines listed below will need to reflect the SQL server name (and instance name if applicable) and the MELD SQL Server login and password created in a previous step.

```
Sub Application_OnStart
  Application("ROOT_URL") = "/MELD"
  Application("IMAGES_URL") = "/MELD/images"
  Application("AppName") = "MELD"
  Application("Physical_Path") = "C:\Inetpub\wwwroot"
  Application("QASP_Option") = 2
  Application("AllowedConcurrentLogins") = 2
  Application("DaysInactiveBeforeBlock") = 35 'DoD requirement is to
  Application("HoursConcurrentReset") = 3
  Application("DaysBeforePasswordChange") = 60 'DoD requirement is to
  Application("AdminTimeOut") = 10 'DoD requirement for an admin us
  Application("CoDE_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
  Application("FEA_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
  Application("Workflow_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeC
  Application("TSSR_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
  Application("CMATT_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
End Sub
```

13.1.2 Application Physical Path

Update the physical path value to reflect the path to MELD on the web server.

```
Sub Application_OnStart
  Application("ROOT_URL") = "/MELD"
  Application("IMAGES_URL") = "/MELD/images"
  Application("AppName") = "MELD"
  Application("Physical_Path") = "C:\Inetpub\wwwroot"
  Application("QASP_Option") = 2
  Application("AllowedConcurrentLogins") = 2
  Application("DaysInactiveBeforeBlock") = 35 'DoD requirement is to
  Application("HoursConcurrentReset") = 3
  Application("DaysBeforePasswordChange") = 60 'DoD requirement is to
  Application("AdminTimeOut") = 10 'DoD requirement for an admin us
  Application("CoDE_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
  Application("FEA_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
  Application("Workflow_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeC
  Application("TSSR_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
  Application("CMATT_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
End Sub
```

Save and close Notepad when complete.

13.1.3 QASP_Option

Refer to the User Guide section “CMATT>Reports>QASP Reports” to determine what reporting method is required for your site. Most sites are using the newest method, option 2. However, older sites are still using option 1.

13.1.4 DoD Settings

The below values set to the default DoD settings with the initial MELD setup. However, if exceptions are approved these setting values can be changed.

13.1.4.1 AuthenticationMethod

The two acceptable values for Authentication Method are “Passcode” or “SmartCard”. If SmartCard is entered a username and password form will be available for first login to the system. After that initial login, the user will automatically authenticate with their CAC.

This value is located within the Application_OnStart section.

Application("AuthenticationMethod") = "Passcode"

13.1.4.2 AllowedConcurrentLogins

The MELD application has set the organization limit to 2 concurrent logins.

This will allow a user to login to MELD twice using the same account, at the same time, for example one instance in Internet Explorer and one instance within Chrome. In order to capture the session data correctly, the user must remember to always log out each time they exit MELD.

This value is located within the Application_OnStart section.

Application("AllowedConcurrentLogins") = 2

13.1.4.3 DaysInactiveBeforeBlock

DoD requirement is to disable an account after 35 days of inactivity.

This value is located within the Application_OnStart section.

Application("DaysInactiveBeforeBlock") = 35

13.1.4.4 HoursConcurrentReset

This value is not a DoD required value, but was added to remove any session data that was not logged out properly after a certain amount of time. The default value is 3 hours. If a user is locked out because of left over concurrent login data within the system, this will automatically clear out after 3 hours. This value can be changed based on the needs of the site and the other values.

13.1.4.5 DaysBeforePasswordChange

DoD requirement is to change a password every 60 days.

This value is located within the Application_OnStart section.

Application("DaysBeforePasswordChange") = 60

August 1, 2021

13.1.4.6 InvalidAttemptsBeforeLock

DoD requirement is to automatically lock a user out after 3 invalid attempts

This value is located within the Application_OnStart section.

Application("InvalidAttemptsBeforeLock") = 3

13.1.4.7 InvalidMinutesBeforeLock

DoD requirement is to automatically lock a user out after 3 invalid attempts within a 15 minute time period.

This value is located within the Application_OnStart section.

Application("InvalidMinutesBeforeLock") = 15

13.1.4.8 TotalCharPassChange

DoD requirement is to require the change of at least 8 of the total number of characters when passwords are changed.

This value is located within the Application_OnStart section.

Application("TotalCharPassChange") = 8

13.1.4.9 TotalPassGen

DoD requirement is to not allow password reuse for a minimum of 5 generations.

This value is located within the Application_OnStart section.

Application("TotalPassGen") = 5

13.1.4.10 PassCharLen

DoD requirement is to have a minimum 15-character password length.

This value is located within the Application_OnStart section.

Application("PassCharLen") = 15

13.1.4.11 PassCharUpperCaseCount

DoD requirement is to have at least one uppercase character.

This value is located within the Application_OnStart section.

Application("PassCharUpperCaseCount") = 1

13.1.4.12 PassCharLowerCaseCount

DoD requirement is to have at least one lowercase character.

This value is located within the Application_OnStart section.

Application("PassCharLowerCaseCount") = 1

13.1.4.13 PassSpecialCharCount

DoD requirement is to have at least one special character.

This value is located within the Application_OnStart section.

```
Application("PassSpecialCharCount") = 1
```

13.1.4.14 PassNumericCount

DoD requirement is to have at least one numeric character.

This value is located within the Application_OnStart section.

```
Application("PassNumericCount") = 1
```

13.1.4.15 DaysBeforeUserPassChange

DoD requirement is to not allow a user to change their password more than once within a 24 hour period.

This value is located within the Application_OnStart section.

```
Application("DaysBeforeUserPassChange ") = 1
```

13.1.4.16 AdminTimeOut

DoD requirement for an admin user is to timeout after 10 minutes of inactivity

Note: If the application pool value was changed to support a larger timeout, then it will need to be reflected here too.

This value is located within the Application_OnStart section.

```
Application("AdminTimeOut") = 10
```

13.1.4.17 Session.Timeout

DoD requirement for a standard user is to timeout after 15 minutes of inactivity

Note: If the application pool value was changed to support a larger timeout, then it will need to be reflected here too.

This value is located within the Session_OnStart section.

```
Session.Timeout = 15
```

13.2 MELD\IME\Web.config

13.2.1 Update Connection Strings

For the IME Web.config, open the file within NotePad and locate the "connectionStrings" section. A typical path to the web.config is located here C:\inetpub\wwwroot\MELD\IME.

```
<connectionStrings>
  <add name="DefaultConnection" providerName="System.Data.SqlClient" connectionString="Data Source=.;Initial Catalog=MELD;Integrated Security=True" metadata="" />
  <add name="CoDEEntities" connectionString="metadata=res://*/CoDEEntities.ssdm;provider=System.Data.SqlClient;providerSettings='Data Source=.;Initial Catalog=MELD;Integrated Security=True';connectionString='Data Source=.;Initial Catalog=MELD;Integrated Security=True' />
  <add name="FEAEntities" connectionString="metadata=res://*/FEAEntities.ssdm;provider=System.Data.SqlClient;providerSettings='Data Source=.;Initial Catalog=MELD;Integrated Security=True';connectionString='Data Source=.;Initial Catalog=MELD;Integrated Security=True' />
  <add name="COIEntities" connectionString="metadata=res://*/COIEntities.ssdm;provider=System.Data.SqlClient;providerSettings='Data Source=.;Initial Catalog=MELD;Integrated Security=True';connectionString='Data Source=.;Initial Catalog=MELD;Integrated Security=True' />
</connectionStrings>
```

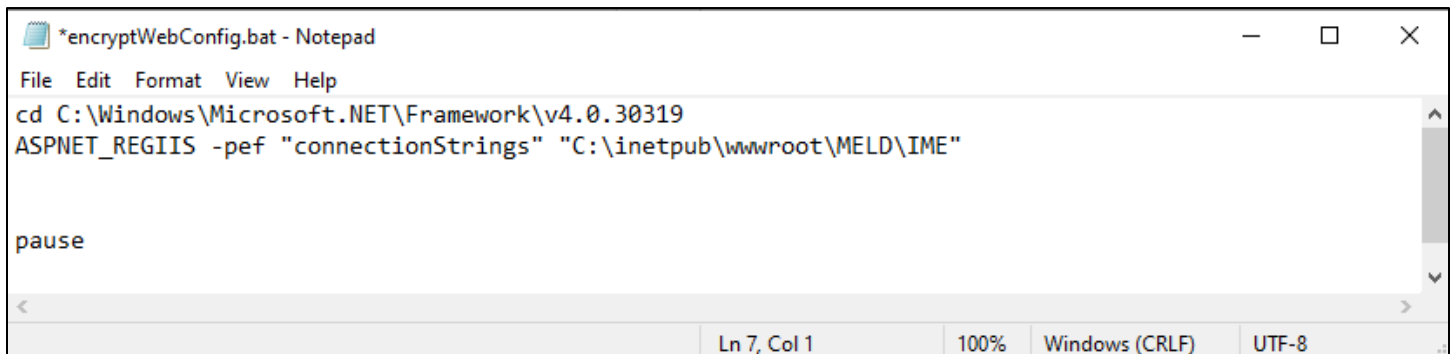
The connection strings will need to reflect the SQL server name (and instance name if applicable) and the MELD SQL Server password created in a previous step.

Save and close Notepad when complete.

13.2.2 Encrypt Connection String

Now that the connection string has been updated to support the SQL server instance and password, it will need to be encrypted to protect the data.

Open the **encryptWebConfig.bat** located within the MELD setup folder and open the file within NotePad. Ensure the path reflects the MELD IME folder located within the wwwroot folder. Update the path if the path is different than what is listed in the file and save the file.



```
*encryptWebConfig.bat - Notepad
File Edit Format View Help
cd C:\Windows\Microsoft.NET\Framework\v4.0.30319
ASPNET_REGIIS -pef "connectionStrings" "C:\inetpub\wwwroot\MELD\IME"

pause
Ln 7, Col 1 100% Windows (CRLF) UTF-8
```

Right click on the file and select **Run As Administrator**.

13.2.3 Update Additional Settings

These additional settings are found within the <appSettings> section of the web.config.

13.2.3.1 SendSiteAdminEmailLogs

MELD will notify system Administrators and Information System Security Officers for all account changes. However, if the MELD server is within a standalone network where email support is not possible, this value should be set to False.

13.2.3.2 SMTPHostServer

The SMTP host will need to be updated to reflect the fully qualified domain name of the web server. If you setup a certificate authority this *information was already identified in an above step*.

*Note: to find the fully qualified domain name for this web server, Select **Control Panel> System and Security>System**. The fully qualified domain name will be listed under **Full Computer Name**.*

13.2.3.3 SMTPHostPort

Note: The DoD accepted port for SMTP is 25. This value should remain as is in the web.config.

13.2.3.4 LogFolderAllocatedSizeMB

The default value for allocated space for the auditing logs is 500MB. This value can be change to meet system preferences. An email will be sent to all system Administrators and Information System Security Officers when 75% of the allocated space is use.

13.2.3.5 LogNonPrivilegeChanges

To allow logging of non-privilege MELD modules such as RIMM and Issue Tracker select this value to true.

14 Setup SMTP on Web Server

Skip this section for standalone MELD web servers that do not have internet access.

This section addresses the DoD requirement to email administrators when account information changes.

To setup SMTP perform the following:

Launch the **Server Manager** and install the **SMTP Server** feature.

14.1 Set Service to Automatic

After the install was successful, select: **Administrator Tools>Services** and locate the **Simple Mail Transfer Protocol (SMTP)** service. Right click this service and select **Properties**. Select the Startup type to **Automatic**. Select Apply.

14.2 Open Port

Contact IT to allow port 25 to and from this web server. *Note: 25 is the DoD approved port for SMTP.*

14.3 mailroot permissions

1. Locate the **mailroot** folder which should be within the InetPub folder.
2. Grant the **Internet Guest Account: IUSR** and the **YourComputerName\IIS_IUSRS** modify, read, and write access to the **mailroot** folder.

14.4 McAfee Settings

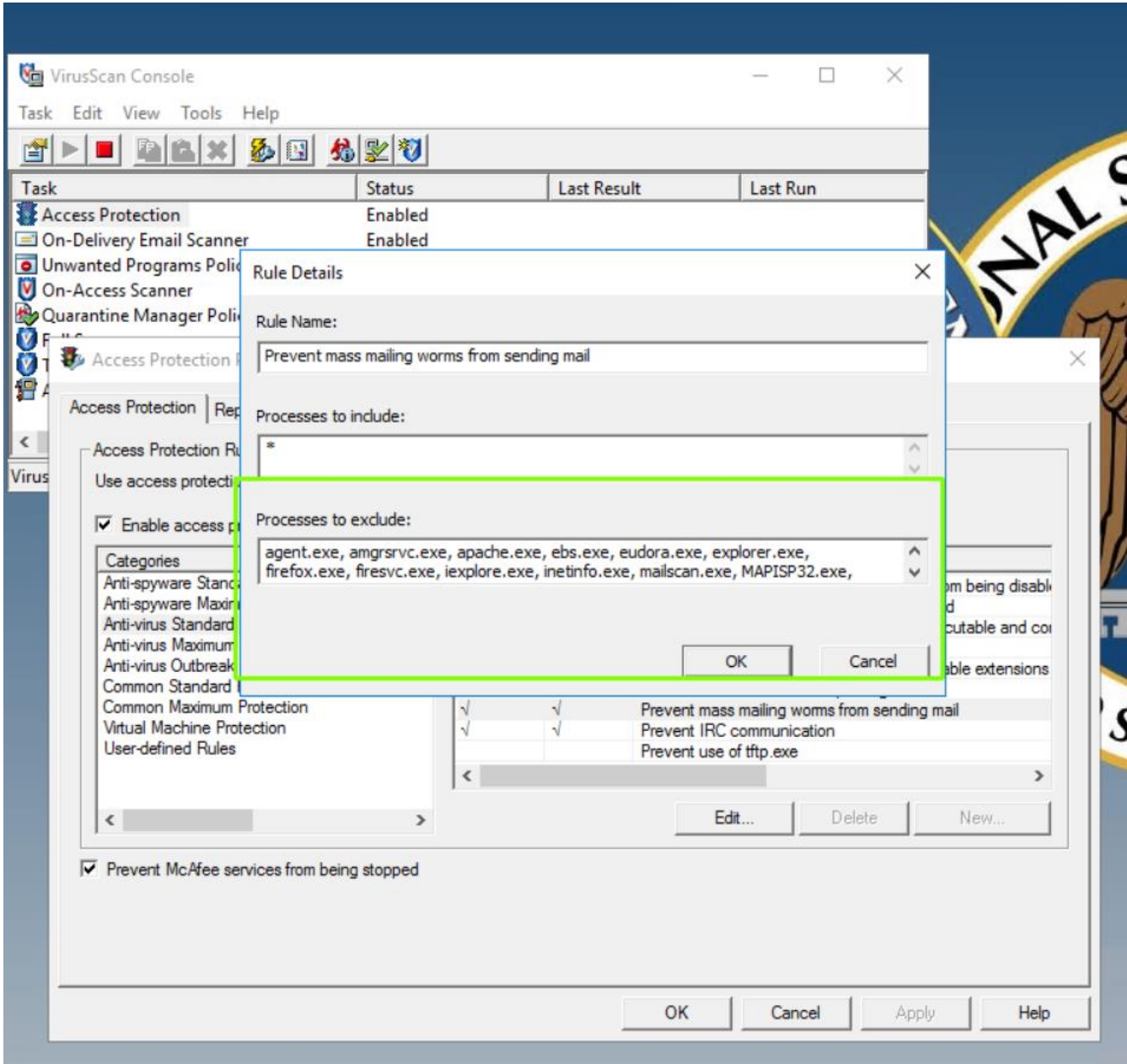
Ensure that McAfee is not blocking the ASP.NET process from sending emails.

1. Open the **VirusScan** Console.
2. Right click on **Access Protection** and select **Properties**
3. Click on **AntiVirus Standard Protection**
4. Single click on “**Prevent mass mailing worms from sending email**”

August 1, 2021

5. Select **Edit**
6. Ensure the following processes are added to the **Exclude** list:
 - w3wp.exe
 - aspnet_wp.exe

Note: These changes may need to be made on the McAfee ePO server if local changes are not allowed or become over written by the McAfee ePO server.



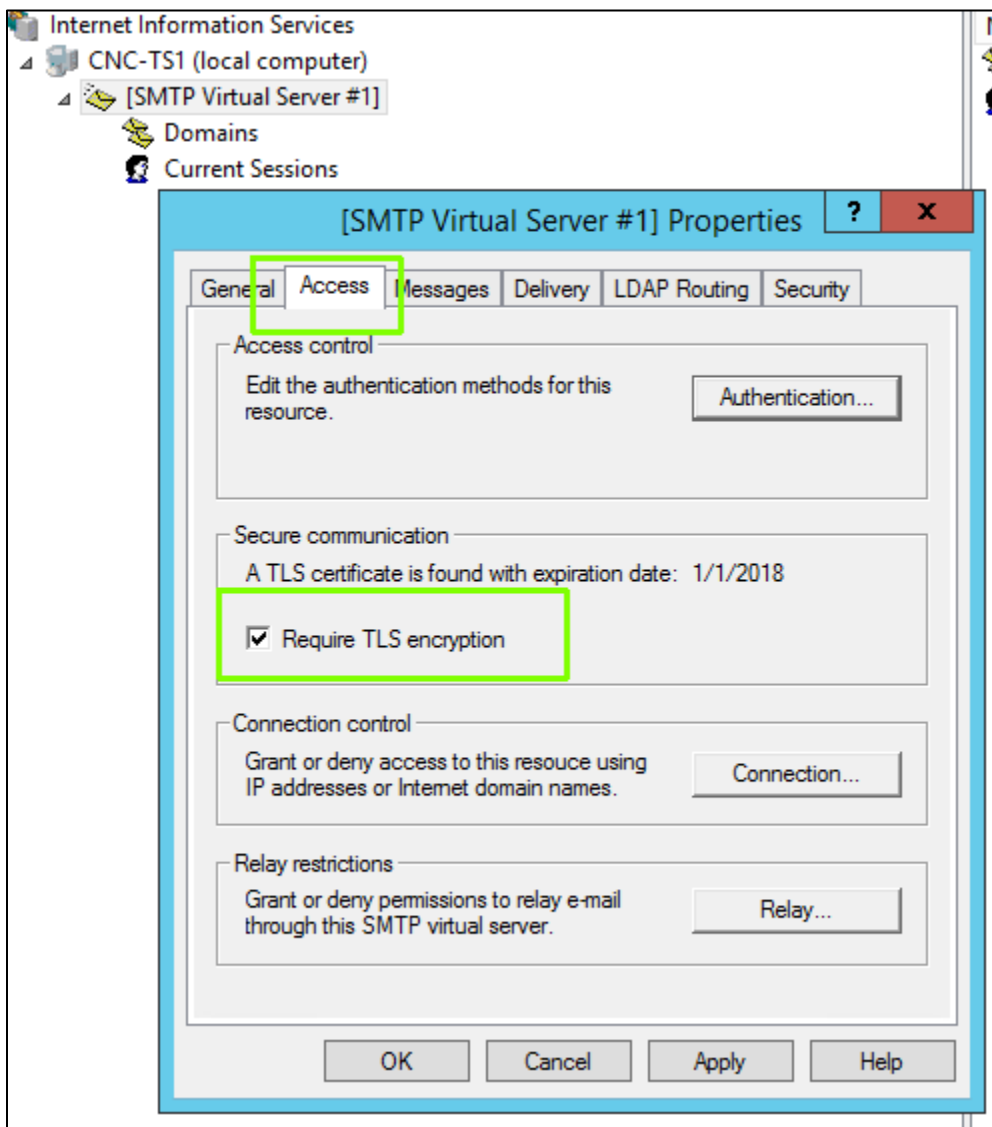
14.5 Launch IIS 6 (installs when the SMTP feature is added)

14.5.1 Require TLS encryption

The DoD requirement is to require TLS encryption, To do this, right click on the SMTP virtual server, select **Properties** and then select the **Access** tab.

Check the box **Require TLS encryption**.

Note: There must be a server certificate located in the Personal folder for the SMTP server (typically the web server). The fully qualified domain name must appear as the common name for the certificate and the certificate cannot use alternative subject names. Refer back to section "DoD SSL certificates" above for more information. If a certificate is not found then the "Require TLS encryption" will not be enabled. Please note the expiration date and ensure the SMTP service is pulling the correct certificate. If it is selecting an expired certificate, then you will need to remove the expired certificates from the Personal folder using the MMC certificate snap in.

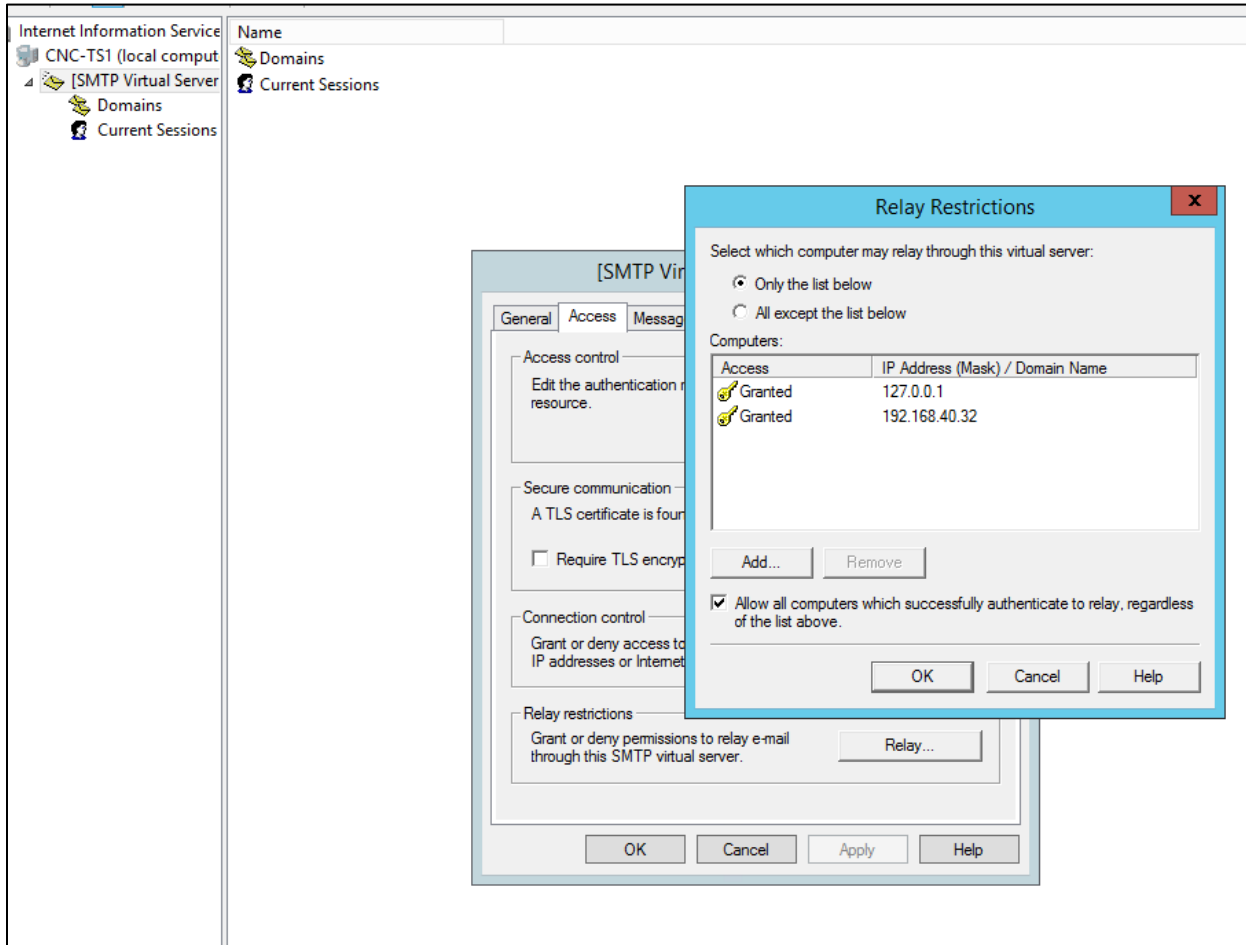


August 1, 2021

14.5.2 Set Relay Servers

On the same access tab, relay restrictions will need to be entered.

1. Select the **Relay** button.
2. Add the following IPs:
 - 127.0.0.1
 - IP of your SMTP server (typically web server)
3. Select **OK**.



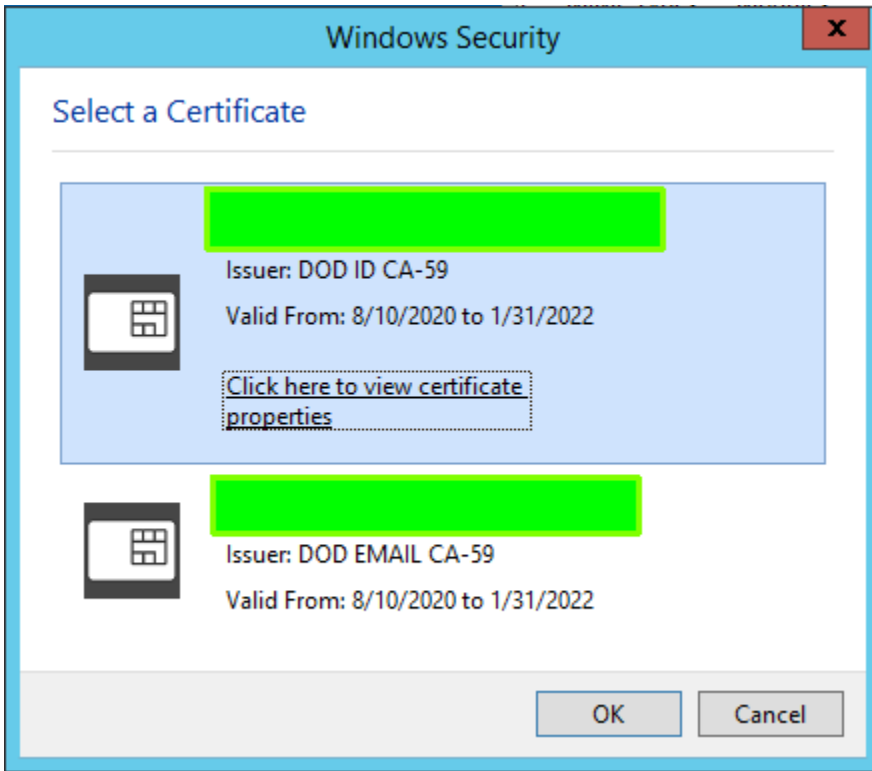
15 Launching MELD

To launch MELD enter the following path within the web browser: Webserver Name or IP/MELD.

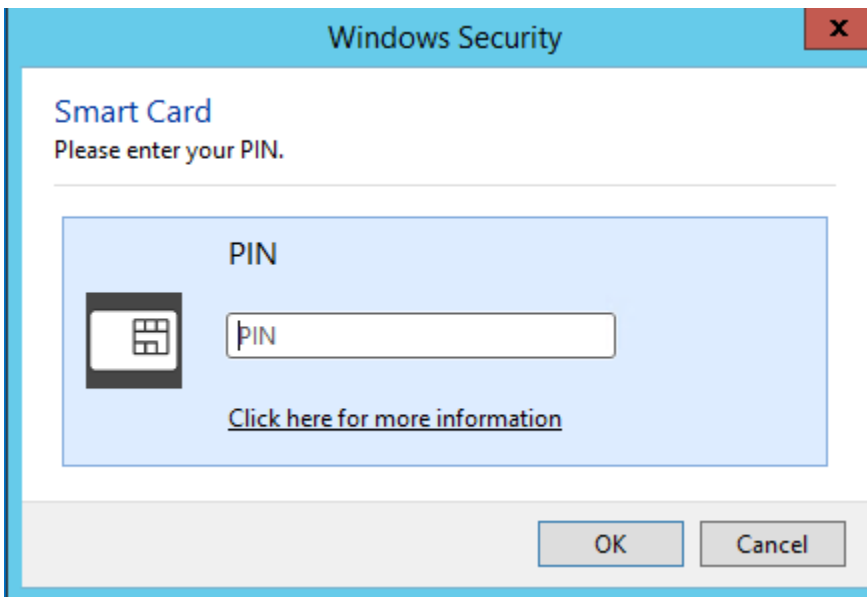
15.1 Initial Launch

15.1.1 Smart Card Systems

For SmartCard systems, before the MELD website will load a certificate popup will display. Select the DoD certificate that is *not* the email certificate, as shown below.



Next, enter the PIN associated with your CAC.



The MELD notice and consent screen will display. Select **I Agree**.

The screenshot shows the top of the MELD application interface. The header includes the MELD logo and the text "Merge, Manage, and Modernize E-Learning Development v3.1". A "CONTACT US" link is in the top right. Below the header is a navigation bar with a "login >" link. The main content area is titled "MELD Notice and Consent Statement". It contains the following text: "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:" followed by a bulleted list of five conditions. At the bottom of the notice, it states: "MELD source code is owned by the USG and therefore no alterations or reproduction of the source in whole or in part, in its current or another format, are authorized." Below this text is an "I Agree" button.

Next a message will display stating that the CAC information did not match the MELD records. Select the **OK** button to login with the initial admin password.

This screenshot is similar to the one above, showing the "MELD Notice and Consent Statement" page. However, a "Message from webpage" dialog box is overlaid in the center. The dialog box has a yellow warning icon and contains the following text: "CAC information did not match the MELD records. Please try to login with your username and password and then try the CAC login again. If you are still unable to access MELD through your CAC login, please contact a MELD administrator to complete the account setup process." Below the text in the dialog box is an "OK" button. The background page content is partially obscured by the dialog box.

August 1, 2021

Enter **admin** for the username

Enter **AdminDefaultAcct!321** for the password

After a successful login, you will need to update the password on the next screen.

This page allows you to change your password. Please note that changes to your information v

Your password has expired

Passwords must meet the following criteria:

1. Cannot be over 60 days old
2. Cannot be one of the last 5 passwords used for this account
3. At least 1 lowercase character: a-z
4. At least 1 uppercase character: A-Z
5. At least 1 number: 0-9
6. At least 1 special character - () ` ~ ! @ # \$ % ^ & * - + = | \ { } [] ; : < > , . ? ()
7. 8 out of the 15 characters in the original password must be changed

Please change your password accordingly.

New Password

Please enter your new password, and click the "Update My Password" button when finished.

Type Old Password:

Type New Password:

Confirm New Password:

Next, select the Administration project and then the User Administration module. Select the **Edit** button within the admin account row, and update the following fields:

August 1, 2021

Login > Projects > Administration > User Administration > Add/Edit Users >

[Reset Password](#)

Add/Edit Users

User Name:
PKI:
Email:
First Name:
Last Name:
Address:
Phone: () - x
Title:
Company/Command:
System Admin:
Security Officer:

- **User Name:** The User Name field needs to reflect a different username than admin. This is typically a combination of a user's first and last names.
- **PKI:** If a PKI value is present then MELD was able to read the PKI from the CAC during the initial login. If no value is present the number on the back of the CAC can be entered.
- **First Name:** The First Name field needs to match the first name exactly as it appears on the CAC.
- **Last Name:** The Last Name field needs to match the last name exactly as it appears on the CAC.
- **Email:** The Email fields needs to reflect the user's email address that should be used for communication.
- **System Admin:** If this MELD account wishes to receive emails when account information is changed, the System Admin drop down will need to change to **True**.

After all fields have changed, select the **Update User** button.

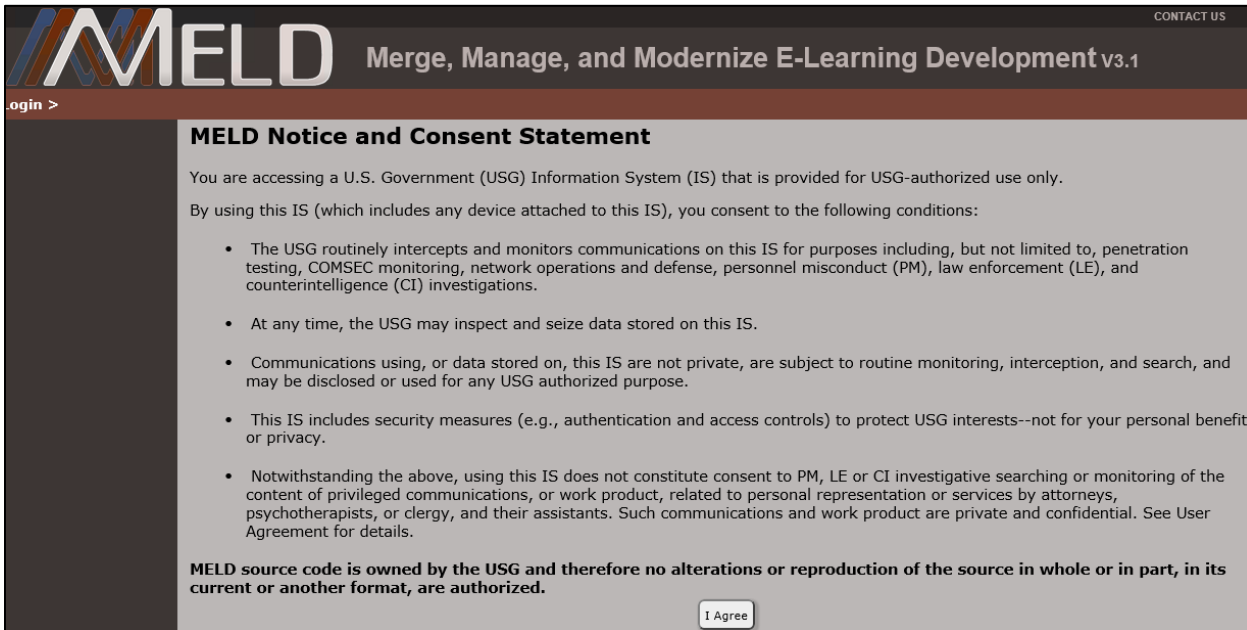
Next, login to MELD again, MELD should recognize your new information and pull it from your CAC and automatically log you in.

It is recommended to create multiple administrator accounts to ensure the system is covered during account lockouts. Refer to the MELD Administrator Guide for more information on creating user accounts.

15.1.2 Username / Password Systems

The MELD notice and consent screen will display. Select **I Agree**.

August 1, 2021



Username and password systems will go directly to the username and password screen.



Enter **admin** for the username

Enter **AdminDefaultAcct!321** for the password.

After a successful login, you will need to update the password on the next screen.

Login > Change Password >

This page allows you to change your password. Please note that changes to your information v

Your password has expired

Passwords must meet the following criteria:

1. Cannot be over 60 days old
2. Cannot be one of the last 5 passwords used for this account
3. At least 1 lowercase character: a-z
4. At least 1 uppercase character: A-Z
5. At least 1 number: 0-9
6. At least 1 special character - () ` ~ ! @ # \$ % ^ & * - + = | \ { } [] ; : < > , . ? ()
7. 8 out of the 15 characters in the original password must be changed

Please change your password accordingly.

New Password

Please enter your new password, and click the "Update My Password" button when finished.

Type Old Password:

Type New Password:

Confirm New Password:

Next, select the Administration project and then the User Administration module. Select the **Edit** button within the admin account row, and update the following fields:

Login > Projects > Administration > User Administration > Add/Edit Users >

Reset Password

Add/Edit Users

User Name:

PKI:

Email:

First Name:

Last Name:

Address:

Phone: () - x

Title:

Company/Command:

System Admin:

Security Officer:

- **User Name:** The User Name field needs to reflect a different username than admin. This is typically a combination of a user's first and last names.

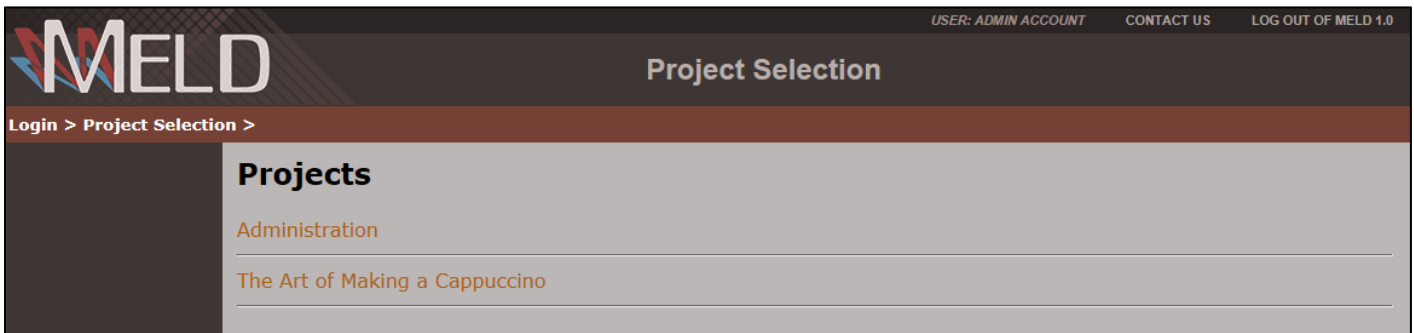
- **First Name:** The First Name field needs to reflect the user’s first name.
- **Last Name:** The Last Name field needs to reflect the user’s last name .
- **Email:** The Email fields needs to reflect the user’s email address that should be used for communication.
- **System Admin:** If this MELD account wishes to receive emails when account information is changed, the System Admin drop down will need to change to **True**.

After all fields have changed, select the **Update User** button.

It is recommended to create multiple administrator accounts to ensure the system is covered during account lockouts. Refer to the MELD Administrator Guide for more information on creating user accounts.

15.2 Project Selection

Two projects will be available. The first project is the Administrator project. The second project is a sample project “The Art of Making a Cappuccino” that contains two sample SCOs.

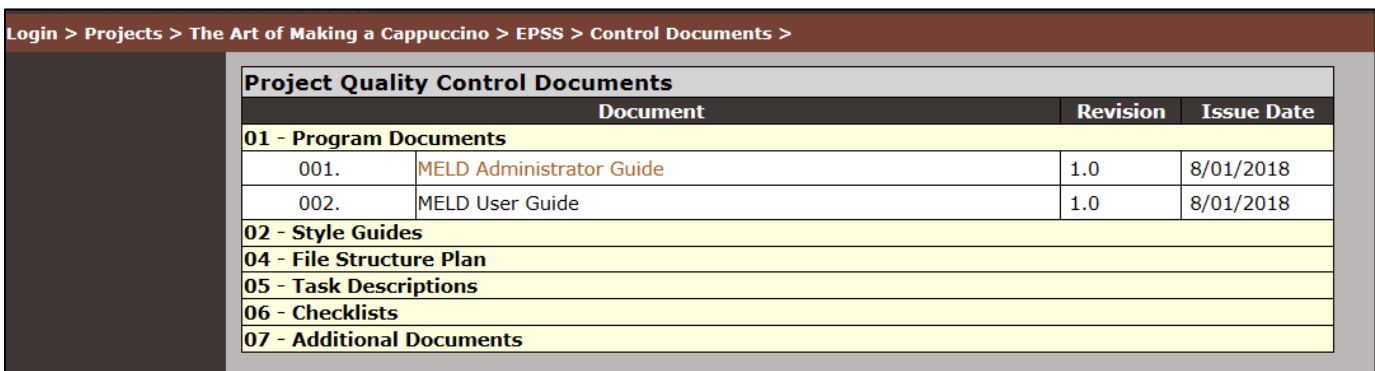


15.3 Browser Support

Follow the “Browser Support” section within the MELD User Manual to ensure all client machines have the correct settings within their internet browser.

15.4 User Guides

Refer to the MELD user guides for additional information for each MELD module. The user guides are available under EPSS>Control Documents for the sample project.



16 System Backups

System backups should be performed daily to ensure all files needed for a disaster recovery are current.

16.1 File System

Ensure the “IME_Data” and the “InetPub” folder are included on the daily file system backup as well as the SQL server backup location listed in the next section. These folders contain the application and all courseware data used within IME. If the site has to perform a disaster recovery, then these folders are needed in addition to the SQL server databases. DoD also requires the IME data logs are off loaded to another location. In the event the backed up logs need to be reviewed, they can be copied back to the IME_Data folder from the backup media and opened within the Log Viewer.

16.2 SQL Server Backups

The SQL Server database files cannot be copied while the databases are active. This prevents a good backup with just the server file system backup. In order to establish a backup of the databases, a backup job will need to be created and ran daily to ensure the MELD data is backed up. SQL Server will write the database backups to a designated folder (for example: D:\SQL_Database_Backups) in the format of a .bak file. The server file system backup routine will then need to back up the .bak files created by SQL Server.

16.2.1 SQL Full Version

MELD databases using the full version of SQL server will need to create a database maintenance plan within SQL Server Management Studio and schedule nightly backups of the 6 MELD databases. It is also recommended to schedule a cleanup routine to remove files after 5 days to prevent the backup folder from getting really large.

The database maintenance plans use the SQL Server Agent to run the backup jobs. Ensure the SQL Server Agent service is running and set to “Automatic” mode to ensure it will run when the server restarts. It is recommended to check daily to ensure the SQL server backups are running and creating the .bak files.

A sample maintenance plan is shown below:

The screenshot displays the SQL Server Enterprise Manager interface. On the left, a tree view shows the server hierarchy, with 'Maintenance Plans' expanded to show the 'KC-130J_Nightly_Backups' plan. On the right, the 'Description' pane shows the details of this maintenance plan, including a subplan named 'Subplan_1'. The tasks within this subplan are:

- Back Up Database (Full)**: Backup Database on Local server connection. Databases: All user databases. Type: Full. Append existing. Destination: Disk. Backup Compression (Default).
- Back Up Database (Transaction Log)**: Backup Database on Local server connection. Databases: All user databases. Type: Transaction Log. Append existing. Destination: Disk. Backup Compression (Default).
- Maintenance Cleanup Task**: Maintenance Cleanup on Local server connection. Cleanup Database Backup files. Age: Older than 5 Days.

16.2.2 SQL Express

MELD databases using SQL Express do not have access to the SQL Server Agent and cannot create a database maintenance plan. The below process can be followed to schedule nightly backups of the SQL server databases:

16.2.2.1 Folder / File Creation

1. Create a folder on the database server hard drive titled **“Database_Backup_Scripts”**. In the below example the D drive is used.

August 1, 2021

2. Create **three** new files within this folder. Notepad can be used to create the file, but make sure to change the file extension from txt to .bat for the first one, .sql for the second and .vbs for the third.

File name: All_Database_NightlyBkUp.bat

```
sqlcmd -S NameOfServer -E -i "D:\Database_Backup_Scripts\All_Database_NightlyBkUp.sql"
REM Run database backup cleanup script
D:\Database_Backup_Scripts\deleteBAK.vbs
```

Copy above text into the file and replace highlighted areas:

- Replace NameOfServer with the name of the server running the SQL express. This will also need to include your instance name, for example: AV8BFS2\SQLEXPRESS.
- Replace D with the drive that you created the Database_Backup_Scripts folder on.

File name: All_Database_NightlyBkUp.sql

- Copy the below text into the file and **create another folder** that will store all the nightly database backups and then replace 'D:\Database_BkUp\' with the path that you created.

```
DECLARE @name VARCHAR(50) -- database name
DECLARE @path VARCHAR(256) -- path for backup files
DECLARE @fileName VARCHAR(256) -- filename for backup
DECLARE @fileDate VARCHAR(20) -- used for file name

-- specify database backup directory
SET @path = 'D:\Database_BkUp\'

-- specify filename format
SELECT @fileDate = CONVERT(VARCHAR(20),GETDATE(),112) +
REPLACE(CONVERT(VARCHAR(20),GETDATE(),108),':','')

DECLARE db_cursor CURSOR FOR
SELECT name
FROM master.dbo.sysdatabases
WHERE name NOT IN ('master','model','msdb','tempdb') -- exclude these databases

OPEN db_cursor
FETCH NEXT FROM db_cursor INTO @name

WHILE @@FETCH_STATUS = 0
BEGIN
    SET @fileName = @path + @name + '_' + @fileDate + '.BAK'
    BACKUP DATABASE @name TO DISK = @fileName WITH NOFORMAT, INIT, NAME = N'db_backup',
SKIP, NOREWIND, NOUNLOAD, STATS = 10

    FETCH NEXT FROM db_cursor INTO @name
END
```

August 1, 2021

```
CLOSE db_cursor
DEALLOCATE db_cursor
```

File name: deleteBAK.vbs

- Replace "D:\Database_BkUp\" with the path that you created to store the nightly backups (created in above step).

```
On Error Resume Next
Dim fso, folder, files, sFolder, sFolderTarget
Set fso = CreateObject("Scripting.FileSystemObject")

'location of the database backup files
sFolder = "D:\Database_BkUp\"

Set folder = fso.GetFolder(sFolder)
Set files = folder.Files

'used for writing to textfile - generate report on database backups deleted
Const ForAppending = 8

'you need to create a folder named "scripts" for ease of file management &
'a file inside it named "LOG.txt" for delete activity logging
Set objFile = fso.OpenTextFile(sFolder & "\scripts\LOG.txt", ForAppending)

objFile.Write "===== " & VBCRLF & VBCRLF
objFile.Write "      DATABASE BACKUP FILE REPORT      " & VBCRLF
objFile.Write "      DATE: " & FormatDateTime(Now(),1) & "" & VBCRLF
objFile.Write "      TIME: " & FormatDateTime(Now(),3) & "" & VBCRLF & VBCRLF
objFile.Write "===== " & VBCRLF

'iterate thru each of the files in the database backup folder
For Each itemFiles In files
  'retrieve complete path of file for the DeleteFile method and to extract
  'file extension using the GetExtensionName method
  a=sFolder & itemFiles.Name

  'retrieve file extension
  b = fso.GetExtensionName(a)
  'check if the file extension is BAK
  If uCase(b)="BAK" Then

    'check if the database backups are older than 5 days
    If DateDiff("d",itemFiles.DateCreated,Now()) >= 5 Then

      'Delete any old BACKUP files to cleanup folder
      fso.DeleteFile a
      objFile.WriteLine "BACKUP FILE DELETED: " & a
```

```

End If
End If
Next

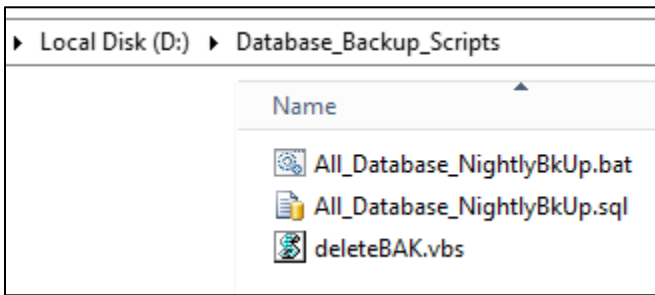
objFile.WriteLine "===== " & VBCRLF & VBCR
LF

objFile.Close

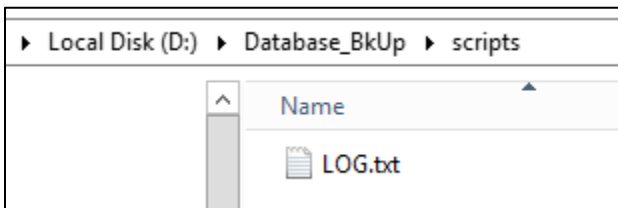
Set objFile = Nothing
Set fso = Nothing
Set folder = Nothing
Set files = Nothing
    
```

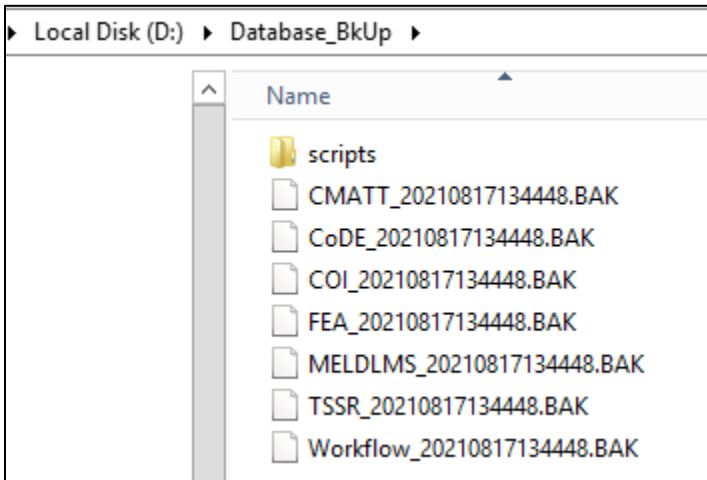
3. Within the nightly backup folder, in this example, "D:\Database_BkUp\", create a "scripts" sub-folder and then create a LOG.txt file within the "scripts" sub-folder. The LOG.txt will create a record of the backup and report any databases that were removed that were over 5 days old.

A sample "Database_Backup_Scripts" folder is shown below:



A sample "Database_BkUp" folder is shown below:





16.2.2.2 Scheduled Task

Create a scheduled task from the Windows task scheduler to run the **All_Database_NightlyBkUp.bat** every evening ~30 minutes before the database server hard drive backup runs. This way the database server backup will catch the database backups within the nightly backup. All databases will be backed up nightly to the backup folder created in the above step. There are 6 MELD databases that should be backing up to this folder and any other databases that are located within the SQL instance.

On the **general** tab for the scheduled task, make sure to run as an account that has permission to back up databases within SQL Server Management Studio. Make sure to select **“Run whether user is logged in or not”** and **“do not store password”**.

August 1, 2021

Create Task

General | Triggers | Actions | Conditions | Settings

Name:

Location:

Author: CNC\mclark

Description:

Security options

When running the task, use the following user account:

Run only when user is logged on

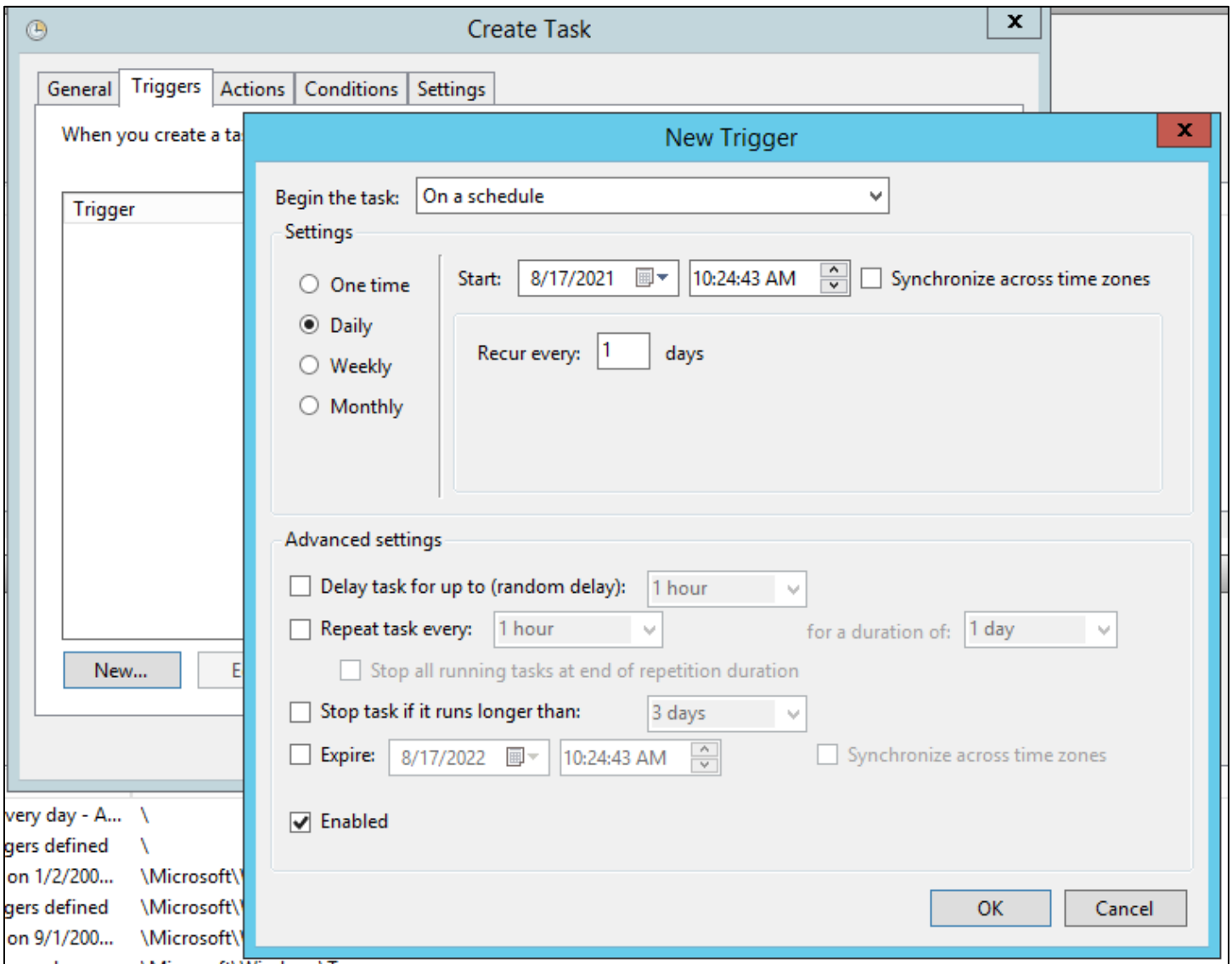
Run whether user is logged on or not

Do not store password. The task will only have access to local computer resources.

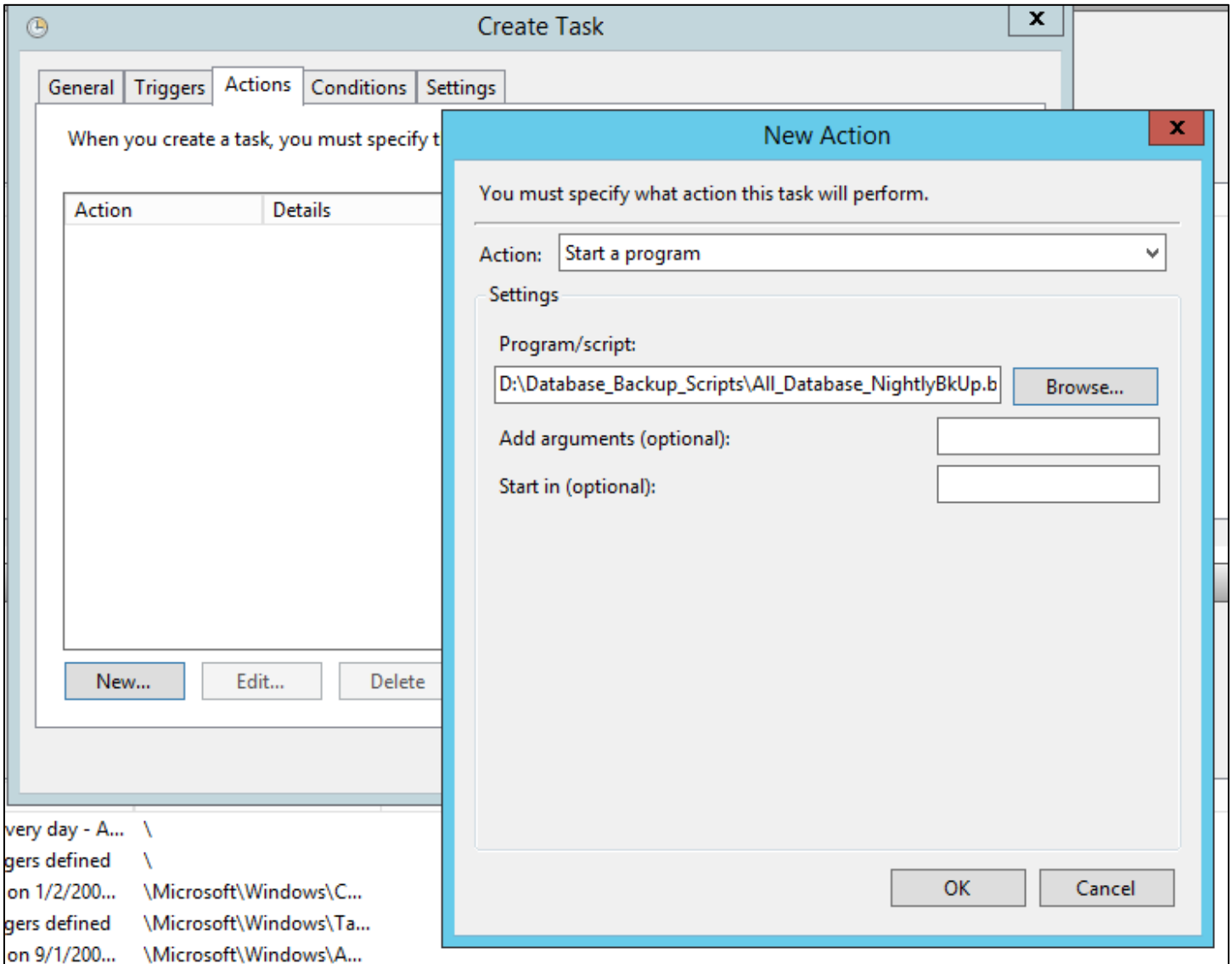
Run with highest privileges

Hidden Configure for:

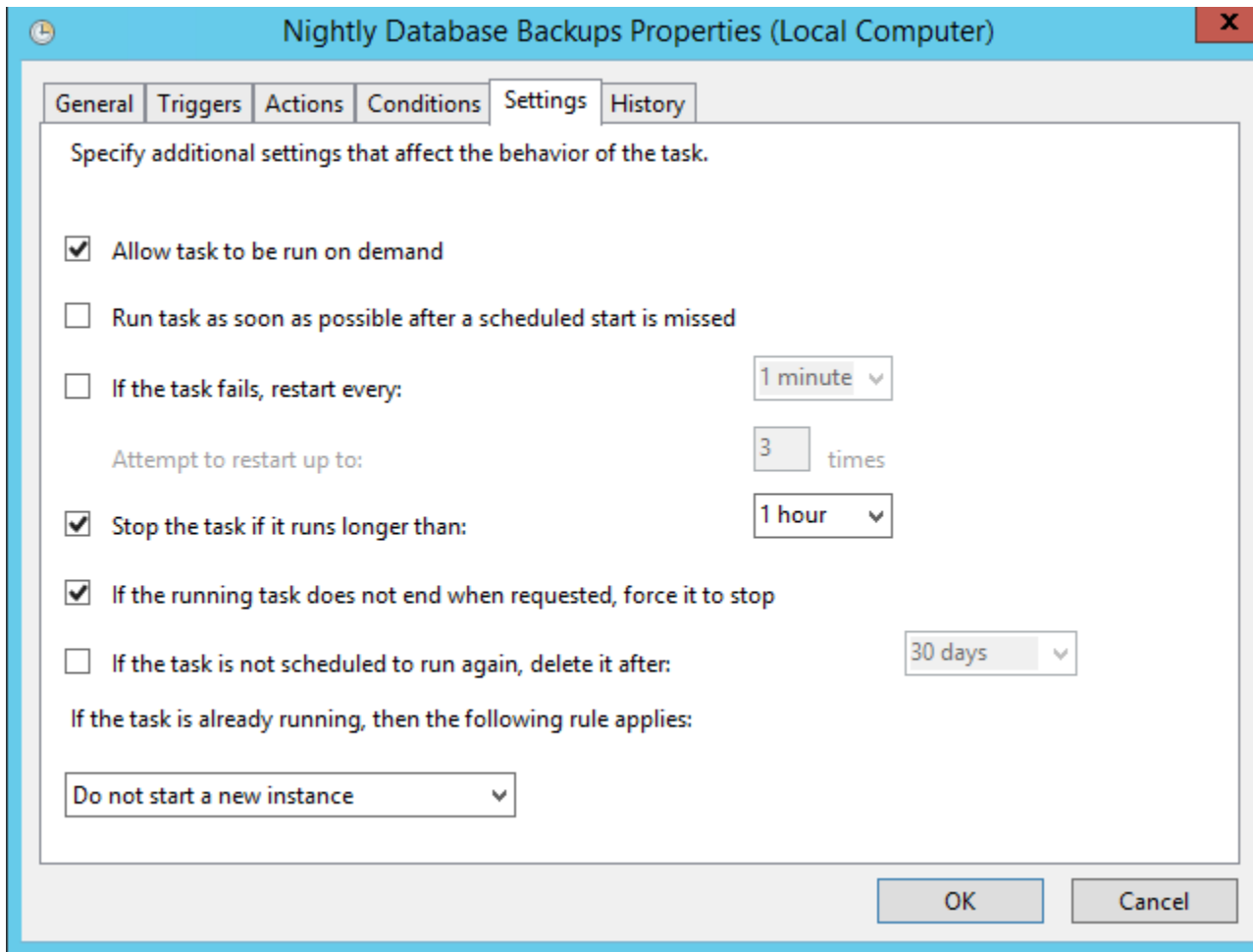
On the **Triggers** tab, select the Daily time for the schedule. This should be around 30 minutes before the server backups run.



On the **Actions** tab, ensure “Start a program” is selected from the Action drop down menu and browse for the **All_Database_NightlyBkUp.bat** file.



On the **Settings** tab, select "1 hour" for the drop down "Stop the task if runs longer than:" Periodically the task will not stop, so the 1 hour selection will ensure the task is stopped and ready to run the following day.



Every morning check to ensure that the database backup from the night before ran. Any backup older than 5 days should automatically be removed. The LOG.txt file created above should document when the backup was performed and what backups were removed.

17 MELD System Maintenance and Security Plan

17.1 Receiving packages from MELD Support

A cryptographic hash function (CHF) is a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size (the "hash value" or "hash "). It is a one-way function, that is, a function which is practically infeasible to invert. By providing a hash value for the MELD installation and update packages, the user can be assured they have downloaded the correct package, with no alterations or data corruption.

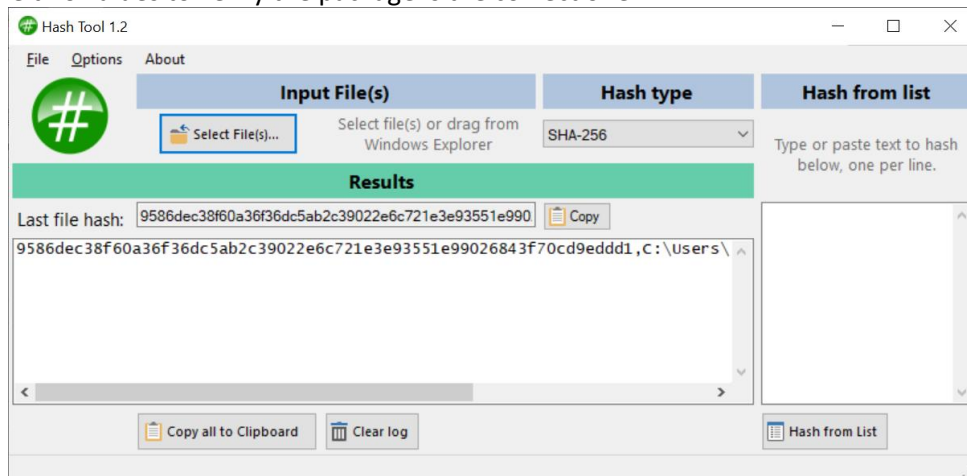
There are a variety of tools that can be used to create a cryptographic hash. These tools will all produce the same output, when using the same algorithm (SHA256, SHA384, etc.). MELD Support uses the Digital Volcano Hash Tool, located at <https://www.microsoft.com/en-us/p/hash-tool/9nblggh4rrr2>, to create the cryptographic hash value. This tool can also be used to verify the hash value of the package.

17.1.1 Update/Installation Package Verification

When creating an update or installation, MELD Support will create and publish a SHA-256 cryptographic hash for the zip file that contains the update or installation. The user can then manually verify this hash value after they have downloaded the update/install, and prior to applying it.

The following steps are based on using the Hash Tool mentioned above. If your site uses a different tool, your steps may vary.

1. Start the Hash Tool
2. Select SHA-256 from the Hash Type dropdown
3. Click on Select File(s) to select the update/installation zip file
NOTE: file selection triggers the hash calculation, so you must have the correct hash type selected first
4. Click on Copy to copy the hash value to the clipboard
5. Paste the hash value into a tool such as Notepad, Word, etc.
6. Paste the provided hash value into the same software (Notepad, Word, etc.)
7. Compare the two values to verify the package is the correct one



17.2 File Server Resource Manager

The DoD requires that the system must alert an administrator when low resource conditions are encountered. To setup alerts the **File Server Resource Manager** feature will need to be installed on the web server.

After the File Server Resource Manager is installed, new quotas can be installed on sensitive folders. The quota size will be determined by the available space on the hard drives and the anticipated size of the project data. The quotas should be set to soft limits that will only sends emails to the administrators when they do reach the limits. The folders will still be operational.

17.2.1 IME_Data quota

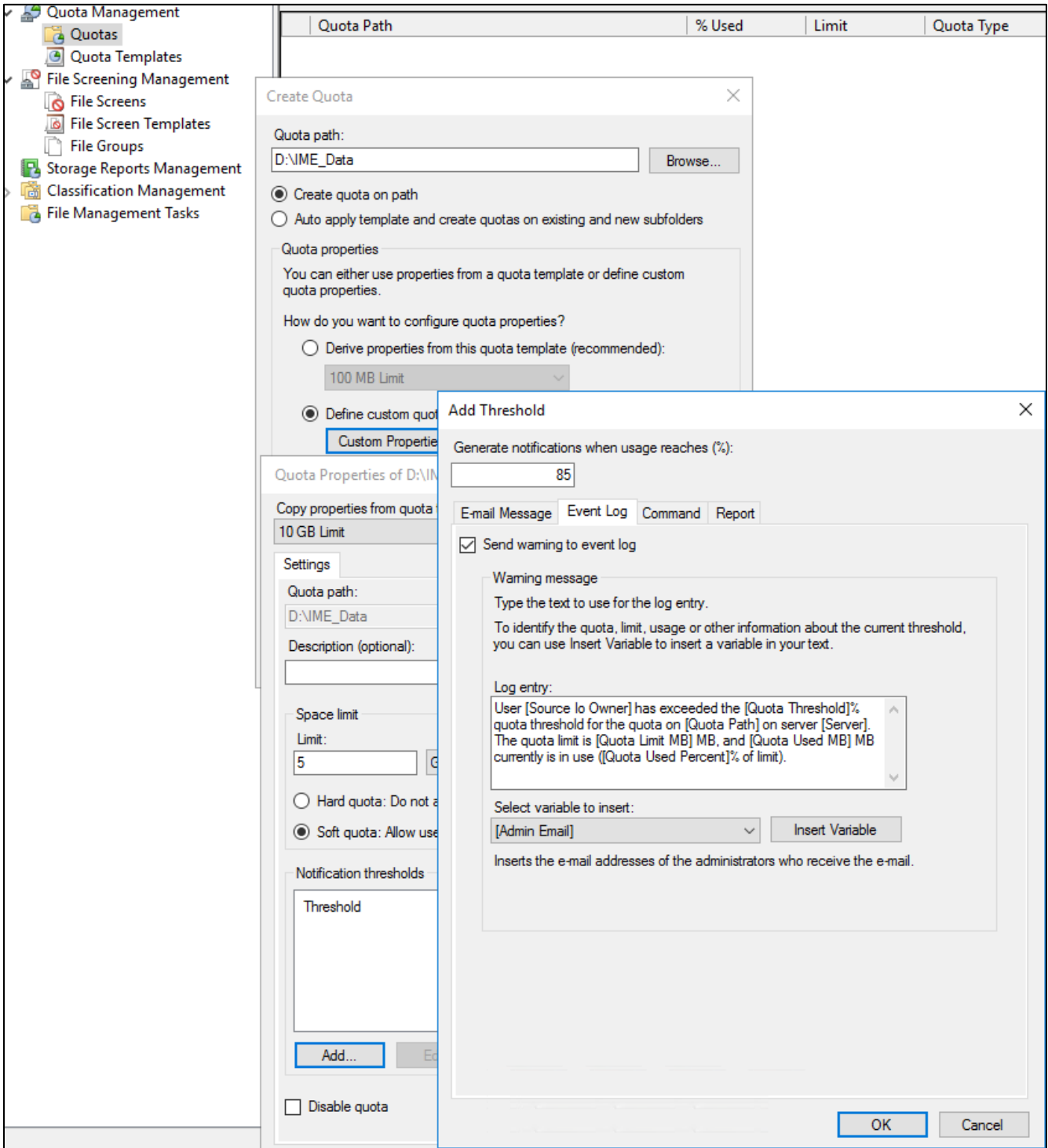
The IME data folder includes all IME courseware, interfaces, and ADL packages created from IME. This folder could get very large depending on the size of the courseware assets and the volume of courseware.

To create a new quota:

1. Right-click on **Quotas** in the treeview and then select **Create Quota**.

August 1, 2021

2. Browse for the **IME_Data** folder for the **Quota path** field.
3. Select the **Define custom quota properties** radio button and then the **Custom Properties....** button.
4. Within the **Limit** field enter the max limit that should not be reached within this folder. The example below uses 5GB, but this value varies per site.
5. Select the **Soft** quota radio button.
6. Select the **Add** button to add a notification threshold
7. Leave 85% for usage
8. Select the Event Log tab and select **Send warning to event log**
9. Select **OK** to close the Add Threshold form.
10. Select **Create** from the Create Quota form.
11. Select **Save the custom quota without creating a template.**
12. Select OK.



August 1, 2021

17.2.2 InetPub folder quota

The inetpub folder contains all web application folders, most likely only the MELD application. Follow the above steps to set alerts for this folder. This folder will not be as large as the IME_Data folder but the limit should be large enough to account for the application logs, application files, and any documents posted to the MELD projects folder.

17.2.3 SQL Server data folder quota

The SQL server data folder contains all MELD databases as well as their transaction log files. Follow the above steps to set alerts for this folder.

17.2.4 Enable SMTP

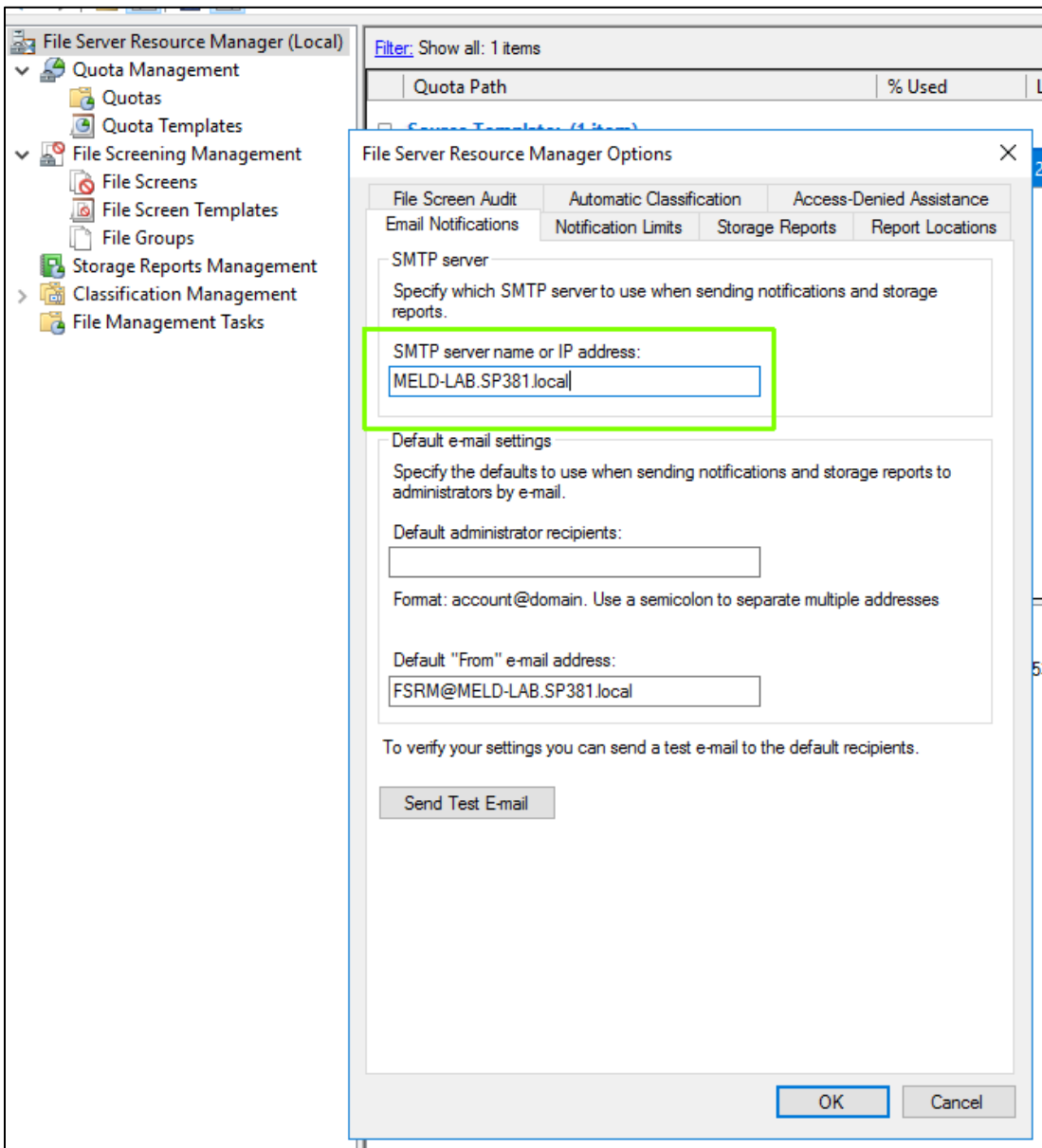
If the antivirus program on the server does not block the sending of emails through the File Server Resource Manager, then email notifications can be setup for the above alerts.

To configure the File Server Resource Manager to send email, right click on **File Server Resource Manager** within the treeview and select **Configure Options**.

Enter the FQDN of the email server.

Next, enter the default email recipient and then click **OK**.

Next, revisit the above quota thresholds and select the E-mail Message tab to add the email notification alert.



17.3 SQL Server Security Plan

17.3.1 Authorized Users

System administrators are the only authorized users for the MELD server. Any other accounts should be removed. System administrators are responsible for keeping the MELD server up to date with DoD standards as well as the MELD application. System administrators should be the only users authorized to perform SQL server updates to the MELD databases, such as stored procedure, table, and trigger updates.

17.3.2 Testing Database Recovery

Testing database recovery should happen at least annually. A desktop can be used to test the database backups. To do this ensure the SQL server express version on the desktop machine matches the version used on the MELD server.

August 1, 2021

Create databases for CoDE, Workflow, FEA, CMATT, and TSSR if not already present on the desktop machine. Restore the databases from the MELD server database backup to the desktop machine and ensure the data restored successfully.

17.3.3 Updating password for meld_user

If DoD enforce password expiration was set for the meld_user SQL server login, or if the password will need to be changed for other reasons, the following configuration files will need to be changed as well.

17.3.3.1 Global.asa

Open the **global.asa** using NotePad within the wwwroot MELD folder and update the connection strings to reflect the new password. A typical path to the global.asa is located here C:\inetpub\wwwroot\MELD.

```
Sub Application_OnStart
    Application("ROOT_URL") = "/MELD"
    Application("IMAGES_URL") = "/MELD/images"
    Application("AppName") = "MELD"
    Application("Physical_Path") = "C:\Inetpub\wwwroot"
    Application("QASP_Option") = 2
    Application("AllowedConcurrentLogins") = 2
    Application("DaysInactiveBeforeBlock") = 35 'DoD requirement is to
    Application("HoursConcurrentReset") = 3
    Application("DaysBeforePasswordChange") = 60 'DoD requirement is to
    Application("AdminTimeOut") = 10 'DoD requirement for an admin us
    Application("CoDE_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
    Application("FEA_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
    Application("Workflow_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeC
    Application("TSSR_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
    Application("CMATT_Connection") = "PROVIDER=MSOLEDBSQL;DataTypeComp
End Sub
```

17.3.3.2 IME web.config

17.3.3.2.1 Decrypt Web Config

To update the IME web.config file, it will first need to be decrypted. To decrypt the file, open the **decryptWebConfig.bat** located within the MELD setup folder and open the file within NotePad. Ensure the path reflects the MELD IME folder located within the wwwroot folder. Update the path if the path is different than what is listed in the file and save the file. A typical path to the web.config is located here C:\inetpub\wwwroot\MELD\IME.

Right click on the file and select **Run As Administrator**.

Now that the web.config is decrypted, open the file within NotePad and locate the "connectionStrings" section.

```
<connectionStrings>
  <add name="DefaultConnection" providerName="System.Data.SqlClient" connectionString="Data Source=.;Initial Catalog=MELD;Integrated Security=True" metadata="" />
  <add name="CoDEEntities" connectionString="metadata=res://*/CoDEEntities.ssdm;provider=System.Data.SqlClient;providerAssembly=System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089;connectionString=Data Source=.;Initial Catalog=MELD;Integrated Security=True" metadata="" />
  <add name="FEAEntities" connectionString="metadata=res://*/FEAEntities.ssdm;provider=System.Data.SqlClient;providerAssembly=System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089;connectionString=Data Source=.;Initial Catalog=MELD;Integrated Security=True" metadata="" />
  <add name="COIEntities" connectionString="metadata=res://*/COIEntities.ssdm;provider=System.Data.SqlClient;providerAssembly=System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089;connectionString=Data Source=.;Initial Catalog=MELD;Integrated Security=True" metadata="" />
</connectionStrings>
```

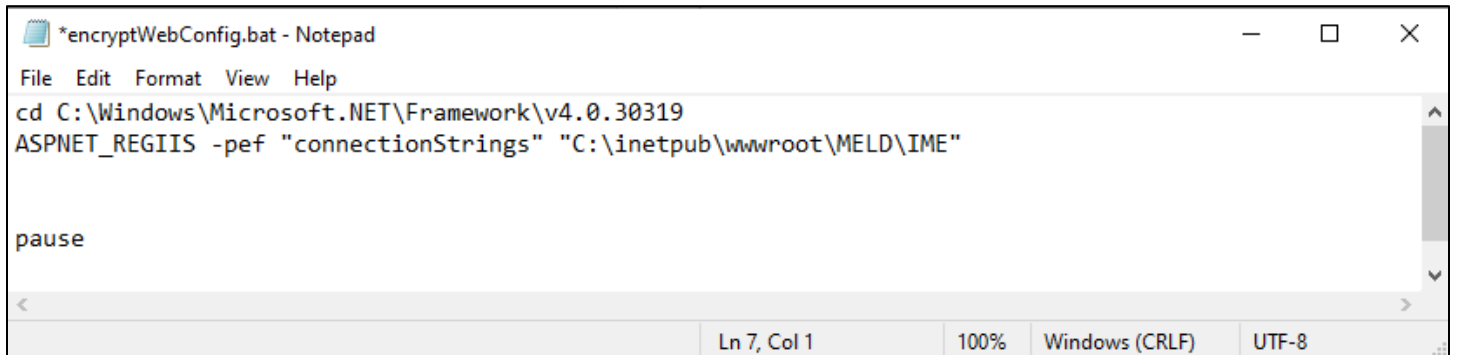
Update each connection string with the new meld_user password.

Save and close Notepad when complete.

17.3.3.2.2 *Encrypt Web Config*

Now, the password has successfully changed, run MELD and then IME and ensure IME opens and retrieves data from the MELD databases. After verification, the IME web.config file can then be encrypted again.

Open the **encryptWebConfig.bat** located within the MELD setup folder and open the file within NotePad. Ensure the path reflects the MELD IME folder located within the wwwroot folder. Update the path if the path is different than what is listed in the file and save the file.



```
*encryptWebConfig.bat - Notepad
File Edit Format View Help
cd C:\Windows\Microsoft.NET\Framework\v4.0.30319
ASPNET_REGIIS -pef "connectionStrings" "C:\inetpub\wwwroot\MELD\IME"

pause

Ln 7, Col 1 100% Windows (CRLF) UTF-8
```

Right click on the file and select **Run As Administrator**.

17.4 IIS Security Plan

17.4.1 DISA revocation lists

In the event that MELD will need to verify the client CAC against the DISA revocation list, the revocation check will need to be enabled.

Please consult with your PM to determine if the revocation list check is necessary for your site and then proceed with the remaining steps in this section if the revocation check is necessary.

17.4.1.1 CRLAutoCache

If determined that the revocation list check is necessary, standalone systems will not be able to load the certificate revocation list on the DISA site and may fail client authentication if a local certificate revocation list cache is not

available. The CRLAutoCache will need to be setup and configured on the web server to enable a cache listing. Please follow the DoD instructions for setup and maintenance.

17.4.1.2 Enable Client Certificate Revocation Check

If determined that the revocation list check is necessary, step “Enable Client Certificate Negotiation” above will need to be performed again, but without the call to disable the client certificate revocation. Reference the table below. This will set the revocation check back to the default value which is to enable the revocation check, while still enabling the client certificate negotiation.

```
netsh http delete sslcert 0.0.0.0:443
netsh http add sslcert 0.0.0.0:443 <cert_hash> {<app_id>} clientcertnegotiation=enable
```

17.4.2 Web Server Certificate Renewal

The web server certificate will expire after a period of time, typically every 1 or 2 years. Before the certificate expires you will need to request a new one, from either your local CA or the DoD. Follow section “DoD SSL certificates” above for obtaining the new certificate. It is recommended to set a reminder to provide enough time to obtain the certificate before it expires.

17.4.2.1 Bind Site to New Certificate

After obtaining the new certificate, launch IIS and select Bindings for the MELD website. Select the binding for port 443 and then select the new certificate.

17.4.2.2 Enable Client Certificate Negotiation

Anytime a new certificate is received, the enable client certificate negotiation must be re-enabled. To do this follow step “Enable Client Certificate Negotiation” within “Configure MELD website for SSL” above. Pay attention to existing client certificate revocation check value *and if that is set to Enabled* then do not include the text to disable it (refer to “Enable Client Certificate Revocation Check” above).

17.4.3 Off load IIS Log Files

IIS logs must be backed up to another location to allow for retrieval in cases where the original logs were removed or altered. A sample location for the IIS logs is: c:\inetpub\logs\LogFiles.

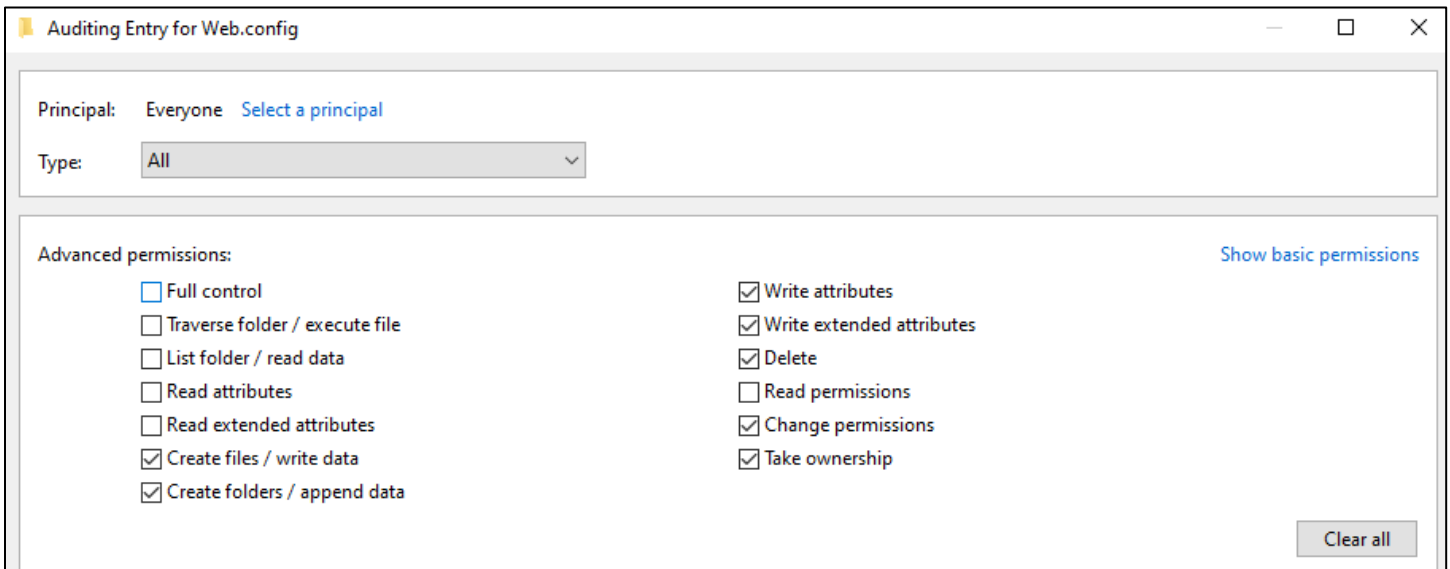
17.4.4 Audit Configuration Files

It is a DoD requirement to audit the MELD global.asa and IME\web.config to identify any unauthorized modifications. To turn on Windows auditing add the following to both of these files:

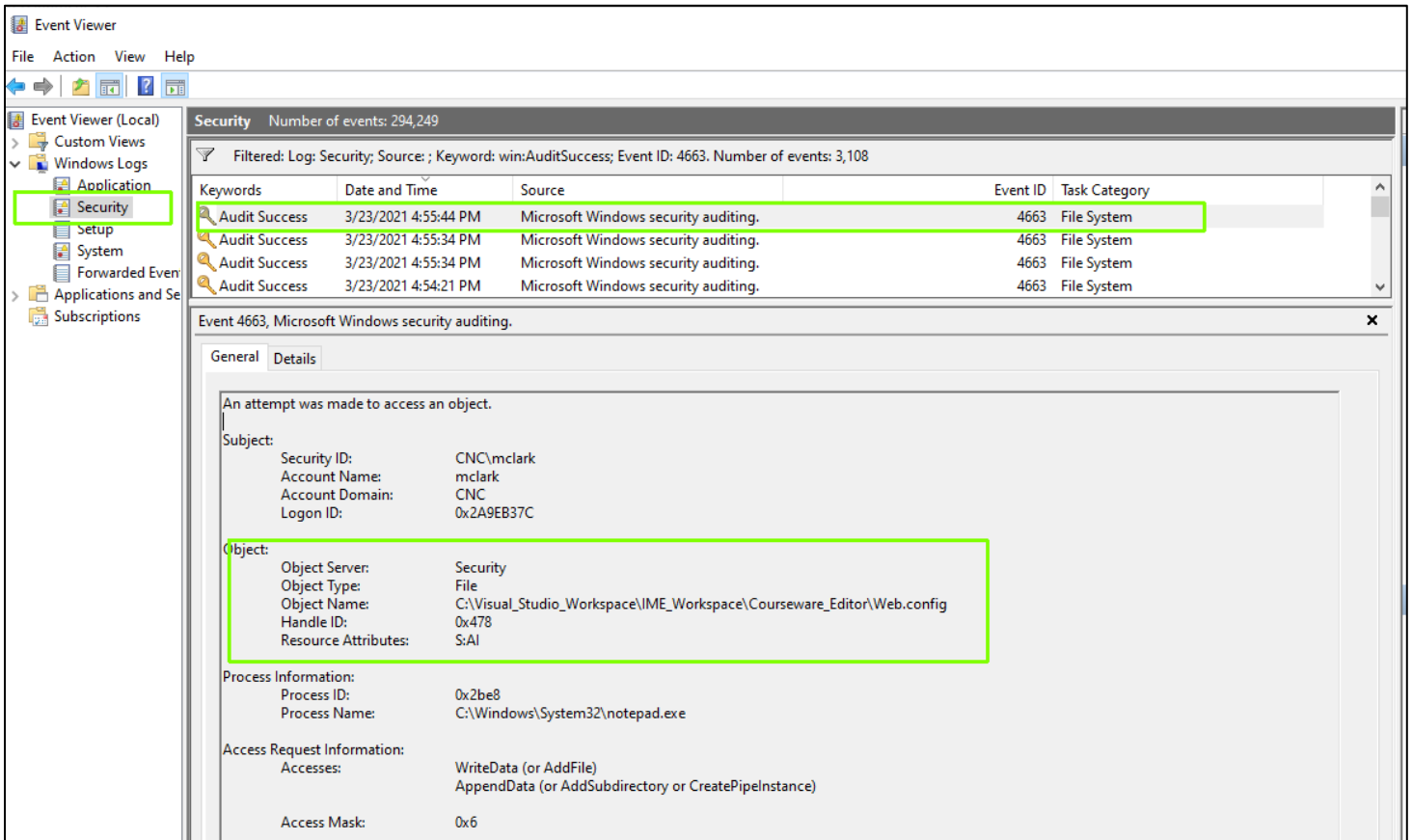
1. Select the **Security** tab and then select the **Advanced** button
2. Select the **Auditing** tab and select Continue as an Administrator (if message appears)
3. Select **Add** to add a new principal
4. Click the **Select a principal** link and add **Everyone** for the object name
5. Select the **show advanced permissions** link
6. Select **All** within the Type dropdown

August 1, 2021

7. **Uncheck** all checkboxes. Since the web service will read these files we don't want to capture those entries and create too many event logs. We only need to capture modifications and deletions.
8. **Check** the following checkboxes to capture modifications and deletions
 1. Create files / write data
 2. Create folders / append data
 3. Write attributes
 4. Write extended attributes
 5. Delete
 6. Change Permissions
 7. Take Ownership



9. Select **OK** three times to close all windows.
10. Now, any changes to this file will be reported within the Event Viewer>Windows Logs>Security with an Event ID of **4663** and Task Category of **File System**.



17.5 Log Folder Maintenance and Rollover

17.5.1 Daily Review

The system administrator should review these log files daily to ensure the application is functioning properly and that no threats have been detected.

11. IIS logs (sample location: C:\inetpub\logs\LogFiles)
12. Windows Event Viewer (application , security, and system logs)
13. MELD logs (sample location: E:\ IME_Data\IME_Logs)

Refer to the below section “Log Browser” for easier viewing of the IIS and MELD logs. The Windows event logs will need to be reviewed within the Windows event viewer to ensure there were no unexpected application changes, shut downs or errors.

17.5.2 MELD Update Log Folder Review and Rollover

During every MELD update, an administrator should review the log folders in the above locations and ensure there is enough space available for additional logs. Log files older than the prior release within the IIS logs as well as MELD logs folder, should be removed or relocated to a different drive. It is a DoD requirement to retain these log files for at least 1 year.

17.5.3 MELD Audit Log Failures

In the event of a MELD audit log failure, email alerts will be sent to all MELD application users listed as a Security Officer or System Admin. The operating system administrator will need to evaluate the system and investigate the failure. If the failure is due to lack of disk space the system administrator will need to relocate older log files to the offload location on a different drive. Files older than one year can be removed. The system administrator will also need to review the MELD IME web.config to ensure enough space is allocated to the log files.

The MELD application does not need to completely shut down due to an audit log failure. However, the system administrator should investigate all audit failures immediately. This level of risk is accepted by the ISSO.

17.6 MELD Account Alerts

It is a DoD requirement that the MELD application notify system Administrators and Information System Security Officers for all account changes. MELD sends the following alerts to any MELD user listed as a Security Officer or System Admin. It is the responsibility of these users to monitor the alerts and investigate any abuse of the system.

- MELD accounts are created
- MELD accounts are modified. This includes any account modification, discipline, and commenting permission changes, and right changes.
- MELD accounts are disabled.
- MELD accounts are deleted.
- MELD accounts are enabled.
- 75% of the allocated audit log space is used.
- Any audit log entry marked as a high or critical event.
- All audit log failures.

17.7 Resuming MELD after a System Failure

If the MELD application fails, due to a system failure or other similar cause, there is no special data required to bring the application back online. Depending on the cause of the failure, it is possible once the application is back online that the status of a user who was active at the time of the failure may have been left in an active state. In these situations there are tools which are described in the MELD Administration Guide that can be used to clear the user session data, allowing them to log back in to the application.

If the system failure is hardware related, IT Staff will replace the failed hardware and restore MELD according to the disaster recovery outlined below.

It is important to review all applicable logs (above section “Log Folder Maintenance and Rollover” contains a list of all available logs) to ensure the system failure was not the result of a threat.

17.8 Shutting Down MELD in the Event of an Attack or Unauthorized Update

17.8.1 Immediate Shut down

To immediately shut down the MELD site, perform the following steps:

1. Open IIS Manager
2. Select the MELD website

3. In the far right under **Manage Website** , select **Stop**
4. If the threat expands beyond the MELD application, repeat for each web site affected.
5. If the threat is at the server level, stop the entire server by selecting the web server instead of an individual site, then select **Manage Server** and then select **Stop**.
6. Review the IIS logs, windows application logs, and the MELD generated logs to investigate any system threats. Refer to the below section “Log Browser” for information concerning the MELD Log Viewer.
 1. IIS logs: Available within the MELD Log Viewer (sample location: C:\inetpub\logs\LogFiles)
 2. Application logs: Available within the Event Viewer (file system path: Windows System Folder\Winevt\Logs\Application.evtx)
 3. MELD logs: Available within the MELD Log Viewer (sample location: E:\ IME_Data\IME_Logs)

17.8.2 Disaster Recovery

To plan for a disaster recovery in the event of a roll back it is important to keep note of the current version of MELD running at the site. MELD is considered a low risk application, and is required by DoD to restore to a working condition within 5 days.

Follow the below steps If there is reason to suspect that the MELD application has been updated by an unauthorized user.

1. Follow the immediate shut down procedures above.
2. Request a release package from the MELD support team of MELD for the MELD version running before shutdown.
3. Permanently remove the MELD directory within the wwwroot folder. A copy of the projects folder within the MELD directly can be backed up to a temp location first.
4. Copy the MELD directory from the release package to the wwwroot location. If the projects folder was copied to a temp location, then move it from the temp location and place it directly into the MELD directory. Refer to section “Update Configuration Files within MELD (File System)” to continue the update.
5. Run a virus scan on all the hard drives within the MELD web server.
6. After the hard drives are checked and do not contain viruses or suspicious files, restore the IME_Data from the server backup as well as the MELD databases (CoDE, FEA, workflow, CMATT, TSSR, and COI) if needed.
7. The websites and server can then be restarted in IIS. In the event the suspicious activity cannot be isolated refer to your company’s disaster recovery procedures for the server.

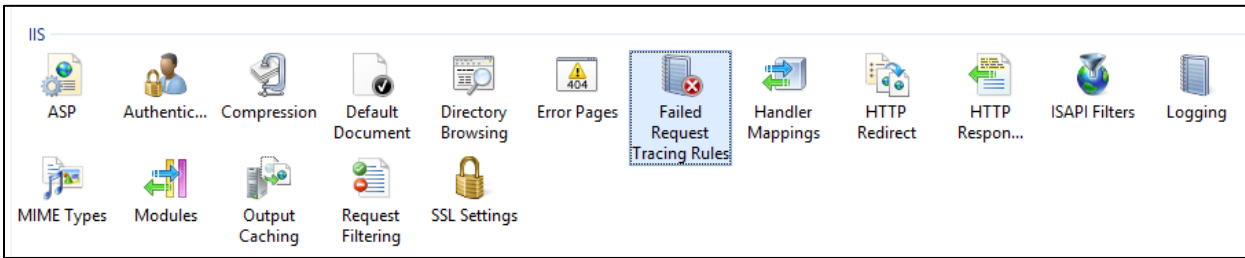
17.9 Troubleshooting Errors on Web Server

17.9.1 Failed Request Tracing

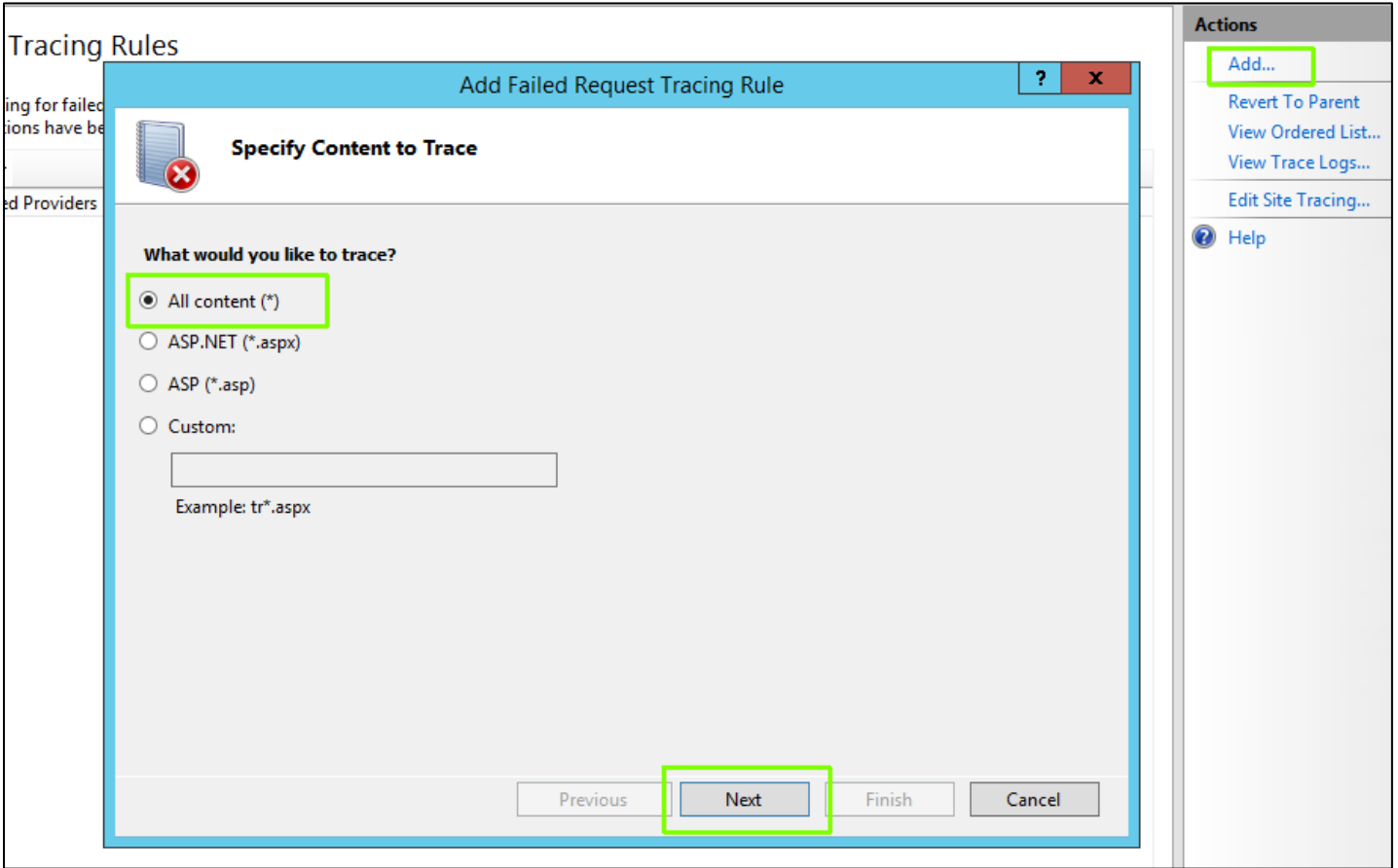
If the application is receiving errors, it is recommended to setup failed request tracing to provide detailed error reporting when the application fails.

To setup failed request tracing:

1. Launch IIS and navigate to the MELD site.
2. Select **Failed Request Tracing Rules**.



3. Select **Add>All content** and then select **Next**.



4. Enter **403,500** for the Status codes. Select **Next** and then **Finish**.

Add Failed Request Tracing Rule

Define Trace Conditions

Under which condition(s) should a request be traced?

Status code(s):

 Example: 401.3-999.405

Time taken (in seconds):

Event severity:

Previous **Next** Finish Cancel

Note: If "Failed Request Tracing Rules" is not available within IIS, the feature will need to be added from Roles and Features within Web Server (IIS) > Web Server > Health and Diagnostics > Tracing

17.9.2 Submitting Log files from Web Server

There are multiple log files that can be sent to MELD Support for further analysis. Please provide data within these locations to MELD Support when an error occurs that requires further troubleshooting.

Setup Errors:

1. Standard IIS log files. A sample location is here: C:\inetpub\logs\LogFiles
2. Failed Request Tracing logs. A sample location is here: C:\inetpub\logs\FailedReqLogFiles

Application Errors:

1. An error_logs table also exists within the CoDE database and can be helpful to MELD Support. The below script can be ran within SQL Studio Management Studio to extract the error logs:

```
Use CoDE
SELECT *
FROM [CoDE].[dbo].[error_logs] ORDER BY date_received DESC
```

2. A logs folder maintains all administrator and session activity and can be helpful to MELD Support. The log files are located here: IME_Data\logs

17.10 Submitting Defects

Defects found by MELD users can be reported to MELD.Support@cti-crm.com.

When a defect is reported, the report should include the following information:

- **Date Raised** - Date when the defect is raised
- **Detected By** - Name, contact information, and company of the person who raised the defect
- **Defect Description** - A detailed description of the Defect including information about the module in which Defect was found.
- **Version** - Version of the application in which defect was found.
- **Steps** - Detailed steps along with screenshots with which the developer can reproduce the defects.
- **Security Vulnerability** - Indicate if the user believes defect is a potential security vulnerability

18 Log Browser

18.1 MELD Audit Logs

All user session logs are written to the log folder on the MELD web server. All events recorded are successful events. If an application occurs while creating an event, the event will be recorded within the error_logs table. The log viewer does not view the records within the error_logs table. A system administrator will need to view the error_logs table separately to view any application errors.

The following user actions are written to the log folder:

User Activity

- Session login time
- Session logout time
- Total time in session
- Concurrent session from two different machines
- Maximum concurrent session limit reached. This is typically set to 2. Refer to “DoD Settings” under section “global.asa” above for configuration settings.
- Browser and IP address used for session.
- Password change
- When a user accesses the file system for lesson, asset, or project logo imports and removals as well as curriculum folder inserts, modifications and removals.

Login Activity

- Invalid login
- Account disabled after allowed number of inactive days. This number is typically 35. Refer to “DoD Settings” under section “global.asa” above for configuration settings.
- Account locked after 3 unsuccessful login attempts.

Privileged Activity

- User account creation
- User account modification

August 1, 2021

- User account locked, unlocked, enabled, disabled, or removed
- User accessing privileged areas that they currently do not have permissions to
- Access and modification to privileged modules:
 - MELD > Administration Project > All modules
 - MELD > Selected Project > Project Administration
 - MELD > Selected Project > IME > Profiles
 - MELD > Selected Project > IME > Settings (Project)
 - MELD > Selected Project > IME > Treeview (curriculum inserts, modifications, or removals)
 - MELD > Selected Project > IME > Selected Lesson > Settings (Editing And Online Review Settings)

Optional Reporting

- Changes made to RIMM module
- Changes made to Issue Tracker module

Refer to “DoD Settings” under section “global.asa” above for configuration settings for optional reporting settings.

18.2 IIS Audit Logs

The following are recorded within the IIS Logs for every page access within the MELD:

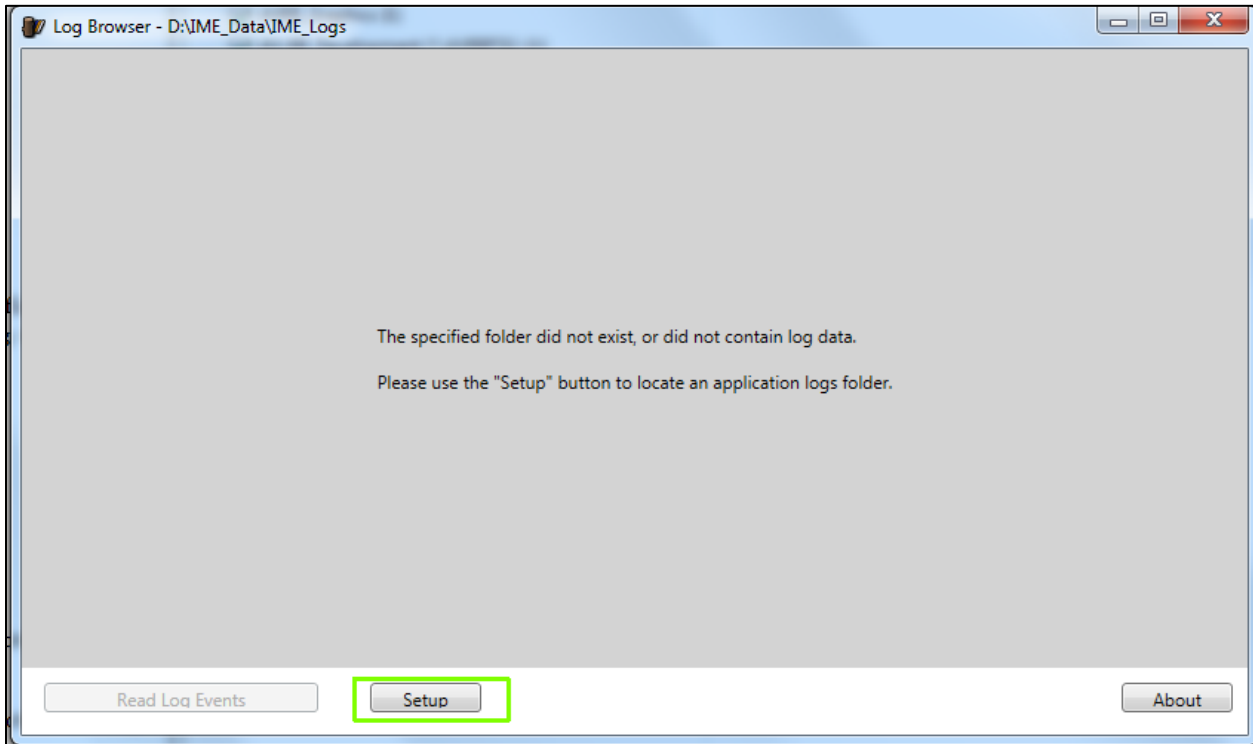
- ASPNET Session ID
- Date / Time
- Client IP Address
- Server IP Address
- Server Port
- Method (GET / POST)
- User Agent
- URI
- Status / Sub Status

18.3 Accessing the Log Browser

Only users that have system administrator privileges to the MELD web server can access the log files. This is not related to the MELD administrator permission within the MELD application. If a user without these privileges needs access to view the log activity, a system administrator for the MELD web server can provide reports for users that do not have access.

The log browser should reside within the IME_Data folder located typically within the D or E drive. Open the Log_Browser.exe that resides directly within the Log_Browser folder.

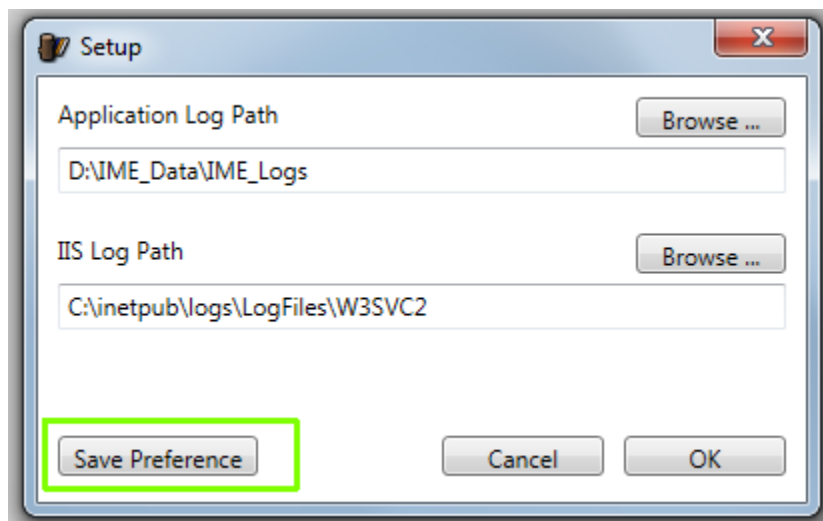
The path to the MELD log directory will need to be setup the first time the application is launched. To setup the log path select the “Setup” button.



Log Browser - Setup

Browse for the directory to the MELD log folder (titled "IME_Logs") located within the IME_Data directory. Also browse for the IIS log folder for the MELD website. An "W3SVC" folder is created for each IIS site and it is important to ensure the correct folder is selected for the MELD site.

After both log files have been updated, select the "Save Preference" button.

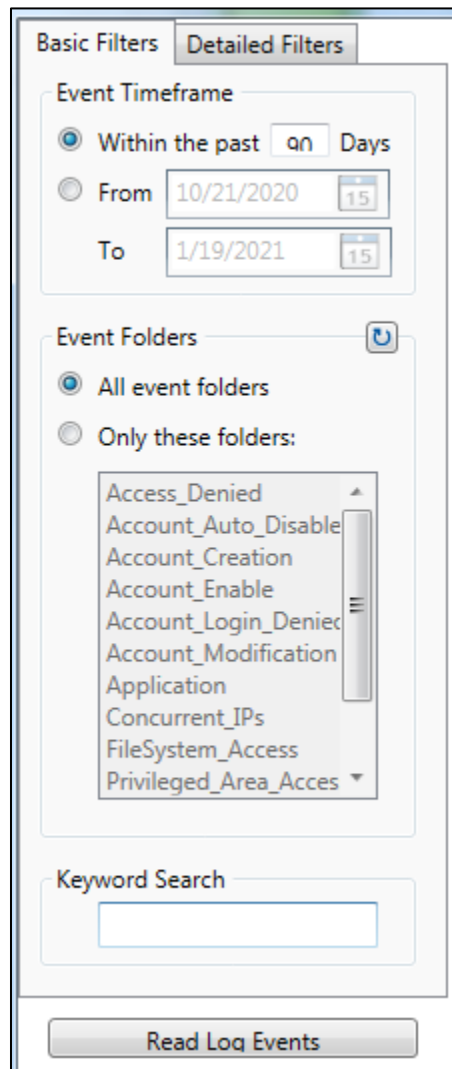


Log Browser – Setup Path

18.4 Read Log Events

Log events can be filtered for basic filters as well as detailed filters. To read specific log events select the desired filters and then select the “Read Log Events” button.

18.4.1 Basic Filters



The screenshot shows the 'Basic Filters' tab of a 'Log Browser' dialog. It features two tabs: 'Basic Filters' (selected) and 'Detailed Filters'. The 'Event Timeframe' section has two radio buttons: 'Within the past 90 Days' (selected) and 'From' (with a date picker set to 10/21/2020) and 'To' (with a date picker set to 1/19/2021). The 'Event Folders' section has a refresh button and two radio buttons: 'All event folders' (selected) and 'Only these folders:'. Below this is a list box containing the following items: Access_Denied, Account_Auto_Disable, Account_Creation, Account_Enable, Account_Login_Denied, Account_Modification, Application, Concurrent_IPs, FileSystem_Access, and Privileged_Area_Access. At the bottom, there is a 'Keyword Search' text box and a 'Read Log Events' button.

Log Browser – Basic Filters

18.4.1.1 Event Timeframe

Select either a data range to search the event logs or enter a value for “within the past x days”.

18.4.1.2 Event Folders

Select the either search all event folders or select the specific event folders to search by single clicking on the folders within the folder listing.

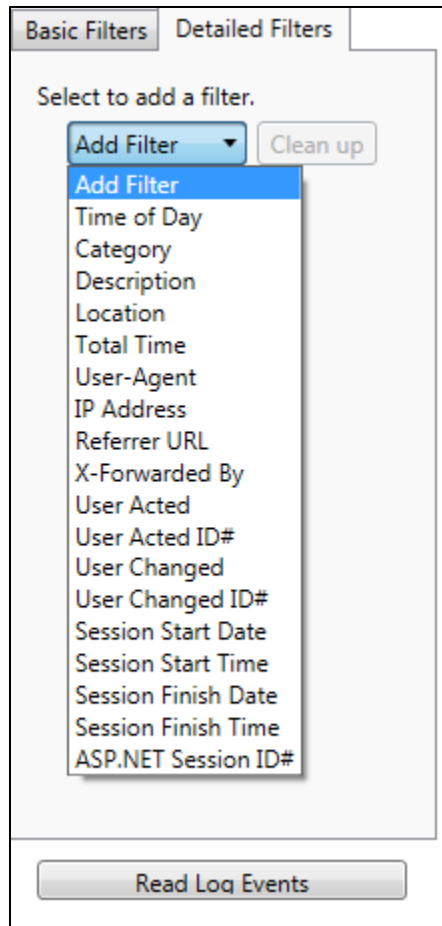
A refresh button is available within the Event Folders header that will create any new folders that previously did not exist when the application was launched.

August 1, 2021

18.4.1.3 Keyword Search

A basic keyword search is available and will search all text fields within the event for the text entered. If any fields match the entered text, the entire event record will be returned.

18.4.2 Detailed Filters



Log Browser – Detailed Filters

18.4.2.1 Add Filter

Select a specific field from the “Add Filter” drop down to add a specific filter. Multiple filters can be added.

18.4.2.2 Clean up

To remove a filter that has already been selected, uncheck the filter checkbox and then select the “Clean up” button.

18.4.3 Event Listing

All events that match the desired filters will display within a table to the right. Single clicking on any event will display the fields below the table for that specific event.

Showing 230 events.
10/22/2020 to 1/20/2021, Event types: All

Local Time	Category	Folder	Description	Location	User Acted
1/5/2021 5:23:37 PM	Warning	FileSystem_Access	Asset Removed: C:\IME\IME_Export\	IME Assets Tab	Clark , Melanie
1/5/2021 5:23:37 PM	Warning	FileSystem_Access	Asset Removed: C:\IME\IME_Export\	IME Assets Tab	Clark , Melanie
1/5/2021 5:23:37 PM	Warning	FileSystem_Access	Asset Removed: C:\IME\IME_Export\	IME Assets Tab	Clark , Melanie
1/5/2021 5:31:46 PM	Information	Privileged_Area_Access	Accessed Privileged Area: Projects >	IME Profile Configuration	Clark , Melanie
1/5/2021 5:31:48 PM	Information	Privileged_Area_Access	Accessed Privileged Area: Projects >	IME Project Settings	Clark , Melanie
1/5/2021 5:31:52 PM	Information	Privileged_Item_Modification	Project Setting: File System Closed cl	IME Project Settings	Clark , Melanie
1/5/2021 5:33:03 PM	Information	Privileged_Area_Access	Accessed Privileged Area: Projects >	IME Project Settings	Clark , Melanie
1/5/2021 5:33:07 PM	Information	Privileged_Item_Modification	Project Setting: File System Closed cl	IME Project Settings	Clark , Melanie
1/5/2021 5:43:29 PM	Information	Privileged_Area_Access	Accessed Privileged Area: Projects >	IME Profile Configuration	Clark , Melanie
1/5/2021 5:44:00 PM	Information	Privileged_Item_Modification	Profile name changed to: Crewmaste	IME Profile Configuration	Clark , Melanie
1/5/2021 6:01:41 PM	Information	Session	Session Ended	System Log Out	Clark , Melanie

Event Detail

Time: 1/5/2021 5:31:46 PM (-05:00)

Category: Information Folder: Privileged_Area_Access

Description: Accessed Privileged Area: Projects > The Art of Making a Cappuccino > Profiles

Location: IME Profile Configuration

Source File: Privileged_Area_Access\2021-01-05_User_1.xml

Users

User Acted: 1 Clark , Melanie

User Changed: (n/a)

HTTP Headers

User Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)

IP Address: 192.168.240.27

Referrer URL: https://cnc-ts1/MELD/IME/default.aspx

X-Forwarded For:

Additional Data

ASP.NET Session: jerwhodjmbcnu3nw4pvybpsd

Session Started: (n/a)

Session Finished: (n/a)

Total Time: (n/a) Minutes

Log Browser – Event Listing

18.4.3.1 IIS Log

An “IIS Log” button will be visible if an IP address was recorded for the event. The IIS log will show all events for the IP address on the day of the selected event. All MELD application traffic is recorded within the IIS log. The time within the IIS log is recorded in UTC time.

MELD Setup and Maintenance Guide 3.1

August 1, 2021

UTC Time	Method	URI Stem	Query	Port	User	User Agent	Referrer	Status	Sub	W32	Time Taken
10:31:39 PM	GET	/MELD/images/IME_refresh.asp	-	443	-	MSIE/7.0	.../projectMenu.asp?...	200	0	0	92 ms
10:31:45 PM	GET	/MELD/.../copy_content.png	-	443	-	MSIE/7.0	.../Profiles.aspx?...	304	0	0	86 ms
10:31:45 PM	GET	/MELD/.../content_logs.png	-	443	-	MSIE/7.0	.../Profiles.aspx?...	200	0	0	111 ms
10:31:45 PM	GET	/MELD/.../add_content.png	-	443	-	MSIE/7.0	.../Profiles.aspx?...	304	0	0	77 ms
10:31:45 PM	GET	/MELD/.../CDOMS.css	-	443	-	MSIE/7.0	.../SessionShare.aspx?...	200	0	0	129 ms
10:31:45 PM	GET	/MELD/.../SessionShare.aspx	UserD=1&TO=10	443	-	MSIE/7.0	.../projectMenu.asp?...	200	0	0	89 ms
10:31:45 PM	GET	/MELD/.../CDOMS.css	-	443	-	MSIE/7.0	.../Profiles.aspx?...	200	0	0	154 ms
10:31:45 PM	GET	/MELD/images/IME_refresh.asp	-	443	-	MSIE/7.0	.../projectMenu.asp?...	200	0	0	75 ms
10:31:45 PM	GET	/MELD/.../enable_disable_treeview.js	-	443	-	MSIE/7.0	.../Profiles.aspx?...	304	0	0	99 ms
10:31:45 PM	GET	/MELD/.../CDOMS.css	-	443	-	MSIE/7.0	.../SessionShare.aspx?...	200	0	0	139 ms
10:31:45 PM	GET	/MELD/.../Profiles.aspx	id=3	443	-	MSIE/7.0	.../default.aspx	200	0	0	402 ms
10:31:45 PM	GET	/MELD/.../SessionShare.aspx	UserD=1&TO=10	443	-	MSIE/7.0	.../projectMenu.asp?...	200	0	0	149 ms
10:31:45 PM	GET	/MELD/images/IME_refresh.asp	-	443	-	MSIE/7.0	.../projectMenu.asp?...	200	0	0	77 ms
10:31:45 PM	POST	/MELD/IME/default.aspx	-	443	-	MSIE/7.0	.../default.aspx	200	0	0	244 ms
10:31:48 PM	GET	/MELD/.../CDOMS.css	-	443	-	MSIE/7.0	.../SessionShare.aspx?...	200	0	0	129 ms
10:31:48 PM	GET	/MELD/.../SessionShare.aspx	UserD=1&TO=10	443	-	MSIE/7.0	.../projectMenu.asp?...	200	0	64	503 ms

UTC Date/Time: 1/5/2021 10:31:45 PM

URI Stem: /MELD/IME/Pages/Profiles.aspx

URI Query: id=3

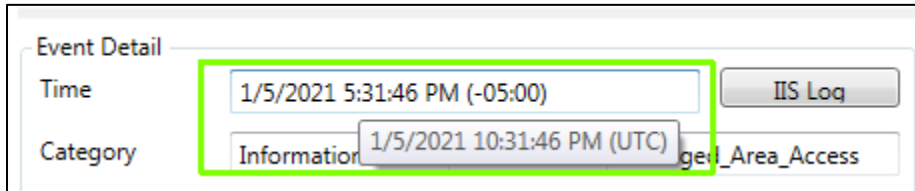
User Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)

Referrer: https://cnc-ts1/MELD/IME/default.aspx

Cookie: ASPSESSIONIDSWATTRQS=FEMDBAHCPGKLIJCBFDBPNN;+ASP.NET_SessionId=jerwhodjmbcnu3nuw4pyybpsd

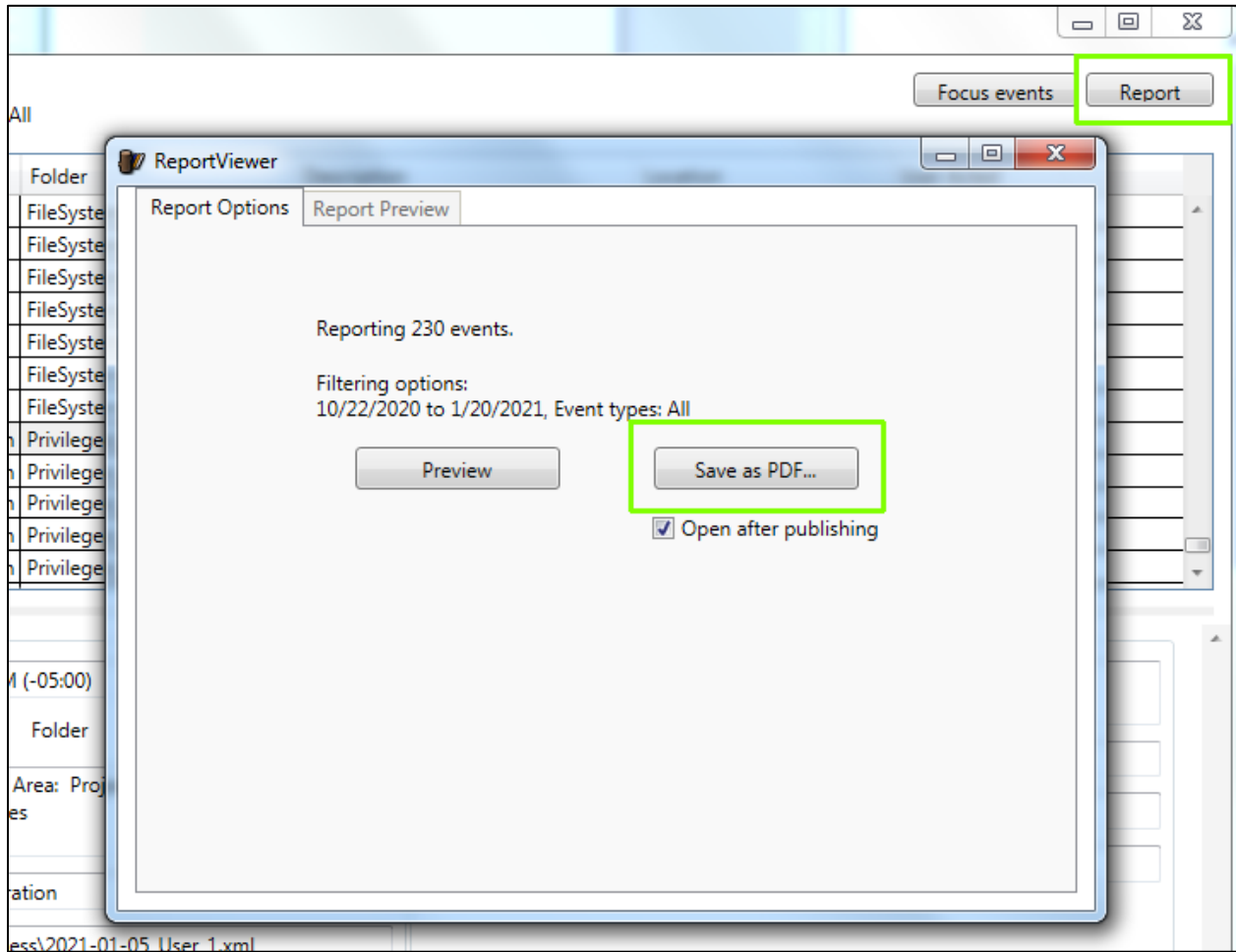
Log Browser – IIS Log

To match the IIS event logs with the MELD application logs you were use the UTC time recorded for the MELD event. To capture the UTC time for the MELD event , hover over the Time field within the Event Detail listing.



18.4.4 Report

Select the “Report button within the top right to print the results to a PDF report. Next select the “Save as PDF” button to save the report to a desired location.



Log Browser – Save Report

Detailed Event Report	
230 events	
10/22/2020 to 1/20/2021	
Event types: All	
<hr/>	
TIME	12/31/2020 11:53:19 AM
CATEGORY	Information
LOCATION	Application Start
EVENT TYPE	Application
DESCRIPTION	Application Started
USER DATA	
USER ACTED	# 0 MELD System
USER CHANGED	(n/a)
<hr/>	
TIME	12/31/2020 11:53:26 AM
CATEGORY	Critical
LOCATION	Login
EVENT TYPE	Account Login Denied
DESCRIPTION	Failed login attempt for user account: ga
USER DATA	
USER ACTED	# 0 MELD System
USER CHANGED	(n/a)
BROWSER DATA	
USER AGENT	Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
IP ADDRESS	::1
URL REFERRER	http://localhost:8050/MELD/_Login/invalid.asp
SESSION DATA	
ASP.NET SESSION ID	3uispmbbbhsrqvcobk1sl01y1

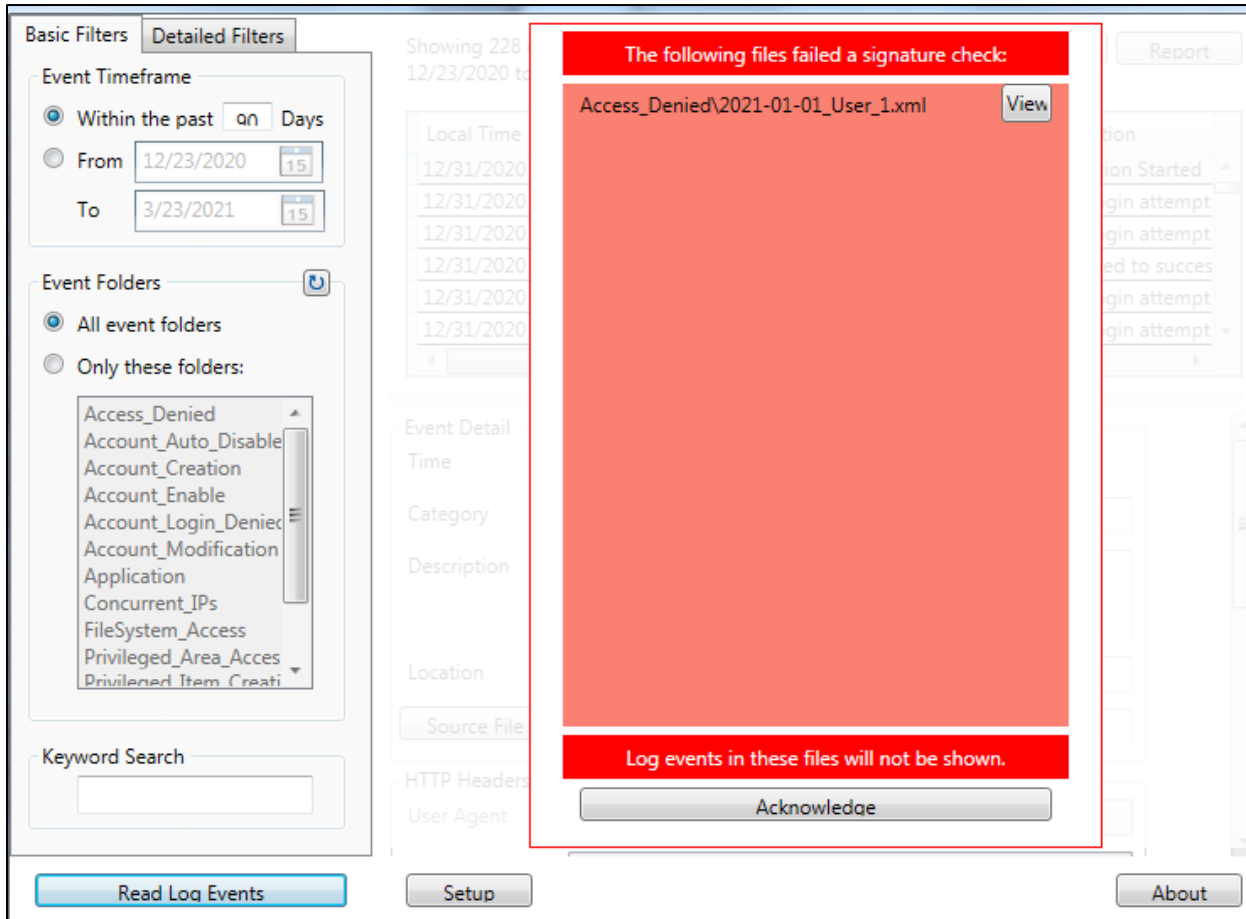
Log Browser – Sample Report

18.5 Audit File Tampering

MELD utilizes the SignedXML class to create an enveloping signature in each audit log file. The signature is verified before additional information can be written to the audit files. If the signature fails an alert will be sent to MELD application Security Officer or System Admin, and a new log file will be created allowing the original file to become investigated.

August 1, 2021

If files were tampered with after the day they were created, the log browser will detect that the signature is invalid and produce the following message:



It is the responsibility of the operating system administrator to investigate the tampering within the identified log files.

19 Sandbox Install

To install MELD in a sandbox / testing environment, the following installation steps within this guide can be skipped.

- 4. DoD SSL certificates
- 5. Install DoD root certificates with InstallRoot (Web Server).
- 9. Configure MELD website for SSL
- 10. Enable HSTS on MELD website
- 14. Setup SMTP on Web Server