

**Digital Certificate User Guide**

**Market Participant Identity Management (MPIM)**

**Version 13**

**May 28, 2020**

Document Revisions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Description | Date | Approved |
| 03/05/2008 | 1.0 | Initial release of the MPIM and Digital Certificate USER’s guide. |  |  |
| 03/17/2008 | 1.1 | Updated for Downloading of Report procedures |  |  |
| 06/11/2008 | 1.2 | Phase II and incorporation of the Protocol 16.12 document “Digital Certificate Introduction and Use For Market Participants |  |  |
| 03/19/2009 | 2 | Revisions and edits |  |  |
| 08/28/2009 | 3 | Phase III Siebel and MPIM Integration |  |  |
| 10/1/2010 | 4 | Phase IV MIS Integration |  |  |
| 11/04/2011 | 5 | Removing TML |  |  |
| 10/30/2012 | 6 | Add entity type: IMRE |  |  |
| 4/01/2014 | 7 | Add a statement about management of multiple Digital Certificates on the same computer, per protocol. | 3/24/14 | dg |
| 9/16/2014 | 8 | Update screenshots – change VeriSign to Symantec  Emails from VeriSign to ERCOT | 9/19/2014 | sa |
| 8/7/2015 | 9 | Update screenshot for renewal email | 8/7/2015 | dg |
| 6/15/2016 | 10 | Add screenshots for email and telephone field and a screenshot to reissue Citrix password | 6/16/2016 | dg |
| 7/11/2018 | 11 | New digital certificate install process  Citrix screenshots | 10/25/2018 | la |
| 10/23/2018 | 12 | Remove 7 day renewal notice | 10/25/2018 | dg |
| 5/28/2020 | 13 | Replace Symantec with DigiCert and added new logo | 5/28/2020 | DL |

**Table of Contents**

[**1. Overview of Guide 4**](#_Toc339373900)

[1.1. Document Purpose 4](#_Toc339373885)

[1.2. Disclaimer 4](#_Toc339373886)

[1.3. Abbreviations 4](#_Toc339373887)

[1.4. MP USA Overview 4](#_Toc339373888)

[1.5. ERCOT will manage Digital Certificates for the MP USA’s 4](#_Toc339373889)

[1.5.1. ERCOT USA will issue the Digital Certificates for the MP USA’s 4](#_Toc339373890)

[1.5.2. How to change or modify MP USA’s 4](#_Toc339373891)

[1.6. Digital Certificate Help 5](#_Toc339373892)

[1.6.1. Additional Resources 5](#_Toc339373893)

[**2. Purpose and Role of Digital Certificates 5**](#_Toc339373894)

[2.1. Digital Certificate Summary 5](#_Toc339373895)

[2.2. What are Digital Certificates? 5](#_Toc339373896)

[2.3. Why does ERCOT use Digital Certificates? 5](#_Toc339373897)

2.4. How is Market System access protected 5

[2.5. Who is DigiCert? 5](#_Toc339373899)

[**3. Getting Started 6**](#_Toc339373900)

[3.1. MP USA Registration 6](#_Toc339373901)

[3.2. I am the USA, now what? 6](#_Toc339373902)

3.3 I received my digital certificate, now what do I do?..................................................................6

[3.4. Distribution for End USER’s 7](#_Toc339373903)

[3.5. Backing up for Unplanned Issues 7](#_Toc339373904)

[3.6. Test Certificates 7](#_Toc339373905)

[3.7. API/Software Certificates 7](#_Toc339373906)

[**4. Market Participant Identity Management Functionality 7**](#_Toc339373907)

[4.1. Assumptions 7](#_Toc339373908)

[4.2. Accessing MPIM 7](#_Toc339373909)

[4.3. Create MPIM USER Account 8](#_Toc339373910)

[4.4. Create Application Programming Interface (API) MPIM Account 10](#_Toc339373911)

[4.5. Certificate Management 11](#_Toc339373912)

[4.5.1. Issue/Reissue USER Certificate in MPIM 11](#_Toc339373913)

[4.5.2. USER Certificate Retrieval 12](#_Toc339373914)

[4.5.3. Viewing Certificate Details 16](#_Toc339373915)

[4.5.4. Lost or Corrupt Certificate 1](#_Toc339373916)8

[4.5.5. Certificate Renewal 1](#_Toc339373917)8

[4.5.6. Revoking USER Certificate in MPIM 20](#_Toc339373918)

[4.6. Modifying a USER and API MPIM Account with Roles 22](#_Toc339373919)

[4.7. Terminating a USER Account 23](#_Toc339373920)

[4.8. Reporting 2](#_Toc339373921)5

[4.8.1. Report Types and Data 2](#_Toc339373922)5

[4.8.2. Downloading the report 2](#_Toc339373923)5

[**5. TSP GATEWAY 2**](#_Toc339373924)**6**

[5.1. USA to assign the role for NMMS to remote USER’s 2](#_Toc339373925)6

[5.2. Reset Citrix Password (Go to Modify in MPIM)…………………………………………………..2](#_Toc339373926)6

[5.3. Email Notification to USER 2](#_Toc339373926)7

[5.4. Citrix Account Creation, Email and Password 2](#_Toc339373928)7

[5.5. Citrix Confirmation Email 2](#_Toc339373930)7

[5.6. Email to Administrator for USER Database Access](#_Toc339373932) 28

[5.7. Logging in to Citrix 1](#_Toc339373937)28

[5.8. USER is required to change password. 30](#_Toc339373938)

[5.9. Access to NMMS and EMS SOTE/MOTE Database 3](#_Toc339373939)0

[5.10. Login Procedures to WEBFG 3](#_Toc339373940)1

[Supporting Reference Documents 3](#_Toc339373942)2

1. **Overview of Guide**
   1. **Document Purpose**

This document provides Market Participant (MP) USER Security Administrators (USA’s) with information regarding the process of receiving their Digital Certificates and serves as a reference tool to navigate through the Market Participant Identity Management (MPIM) features.

* 1. **Disclaimer**

This USER’s Guide provides a general overview of the process for obtaining and handling Digital Certificates. If any conflict exists between this USER’s Guide and the ERCOT Protocols, then the ERCOT Protocols shall prevail. Please refer to the ERCOT Protocols “*USER Security Administrator and Digital Certificates*”, Section 16, regarding complete details of USA responsibilities.

* 1. **Abbreviations**
* EDC – ERCOT Digital Certificate
* ERCOT – Electric Reliability Council of Texas
* ERCOT USA – ERCOT USER Security Administrator
* MP – Market Participant
* MPIM – Market Participant Identity Management
* MP USA – Market Participant USER Security Administrator
* NCI – Notice of Change of Information
* USA – USER Security Administrator
* MIS – Market Information System
  1. **MP USA Overview**

Each MP must appoint an MP USA and has the option to register a secondary MP USA. ERCOT encourages the use of a secondary MP USA to prevent the loss of ERCOT system functionality in the event the primary MP USA is unavailable or leaves the company. MP USA registration is part of the initial MP registration process. The MP USA is responsible for managing the entire Digital Certificate process for their company. The MP USA is responsible for coordinating Digital Certificate requests and maintaining USER roles and access to ERCOT systems.

For assistance with registering a new MP USA or changing MP USA contact information, please visit <http://www.ercot.com/services/rq/index.html> and follow the instructions on the Notice of Change of Information (NCI) form.

* 1. **ERCOT will manage Digital Certificates for the MP USA’s**
     1. **ERCOT USA will issue the Digital Certificates for the MP USA’s**

1. Once ERCOT has received management approval of a new Market Participant qualification or an NCI form, ERCOT will begin the process of issuing Digital Certificates for the MP USA(s).
2. The MP USA(s) will receive two emails. One will contain a URL to access the login page along with the employee id, and the second will contain a password and DUNS number.
3. Once your Digital Certificate is installed, the USER’s Guide is available by clicking on “Support Documentation” via the homepage of the MPIM system.
   * 1. **How to change or modify MP USA’s**
4. To change the MP USA or to modify their contact information, please visit <http://www.ercot.com/services/rq/index.html> and follow the instructions on the Notice of Change of Information (NCI) form.
5. Once ERCOT has received approval of the NCI form, Client Services will send notification to the ERCOT USA to issue a digital certificate(s) via the MPIM system.
   1. **Digital Certificate Help**
      1. **Additional Resources**

* To report technical issues or for help on topics not covered in this guide, you may contact the ERCOT Helpdesk at (512) 248-6800. *Please provide the following information:*
* **Market Participant’s DUNS number**
* **Employee ID(s) in question**
* **Exact name on the digital certificate**
* Any other questions regarding contacts or account information, please contact your ERCOT Account Manager or Client Services at 512-248-3900. Please be prepared to provide the same information listed above.

1. **Purpose and Role of Digital Certificates**
   1. **Digital Certificate Summary**

A Digital Certificate is an electronic "passport" that establishes your credentials when doing business or other transactions on the Internet. A Digital Certificate is a security measure installed on a USER’s computer to identify the person to ERCOT. Digital Certificates are used to access ERCOT systems and ensure that connections are secure. DigiCert administers all ERCOT Digital Certificates. For more information on DigiCert, please visit their website at https://www.digicert.com

* 1. **What are Digital Certificates?**
* Digital Certificates identify each USER to ERCOT, and without a Digital Certificate, access is declined.
* Digital Certificates provide a “digital signature” that tells the recipient, in this case ERCOT, that the information actually came from the sender and has not been forged or tampered with.
* Digital Certificates provide access to web sites identified by https://. The “s” in the address identifies the site as a “secured” site.
* Digital Certificates are installed on the USER’s PC and are utilized by the web browser. A USER must use the PC on which the Digital Certificate is installed to access any secured site at ERCOT.
* MIS also known as the Portal and MarkeTrak (MT) are examples of secure ERCOT systems.
* Digital Certificates ensure that you are accessing the actual ERCOT site to prevent “spoofing.” This means someone could create a false site where companies could enter sensitive and confidential information.
  1. **Why does ERCOT use Digital Certificates?**
* ERCOT uses Digital Certificates to associate an identity with a USER.
* ERCOT uses Digital Certificates to secure private information from the public.
* In addition, Digital Certificates secure private information from other MPs.
* Digital Certificates provide a transparent logon to ERCOT systems. No USER ID or password is required to enter a transparent site.
  1. **How is Market System access protected?**
     + - A Digital Certificate is intended for use by only one USER and is not to be shared among USER’s.
       - If multiple employees or authorized agents share a computer and each requires a Digital Certificate, the USA shall request separate Digital Certificates for each user. Multiple Digital Certificates may be installed and managed on a single computer.
       - Personal computers should be secured appropriately (screensaver passwords, etc.) to prevent improper use.
       - The MP assumes liability if these guidelines are not followed by anyone in the MP’s organization.
       - A yearly audit is conducted to keep ERCOT’s Digital Certificate database information current and accurate. For more information on ERCOT’s annual audit, please see Protocol Section 16.12:3 “USER Security Administrator and Digital Certificates”.
  2. **Who is DigiCert?**
* DigiCert manages Digital Certificates for all MPs.
* DigiCert’s functionality provides secure internet access, certificate validation, and automated certificate renewal among other functions.
* DigiCert will correspond with MPs via email concerning Digital Certificates.
* To view DigiCert’s homepage go to <https://www.digicert.com>

1. **Getting Started**
   1. **MP USA Registration**

After an MP completes the registration application in accordance with the ERCOT Protocols, the ERCOT MPIM administrator will enroll the new USA in MPIM. Upon completion of registration and any necessary qualification, the ERCOT Account Manager for that MP will send a request to have the MP USA production Digital Certificate authorized. ERCOT’s managing staff reviews and approves the request for DigiCert to issue the MP USA production certificate as one of the following types of entities (this includes sub-entities):

* LSE (Load Serving Entity)
* ELSE (External Load Serving Entity)
* QSE (Qualified Scheduling Entity)
* CRRAH (Congestion Revenue Rights Accountholder)
* CP (Counterparty)
* TDSP (Transmission and Distribution Service Provider)
* TSP (Transmission Service Provider)
* DSP (Distribution Service Provider)
* FERC (Federal Energy Regulatory Commission)
* NERC (National Energy Regulatory Commission)
* RE (Resource Entity)
* PUCT (Public Utility Commission of Texas)
* TRE (Texas Reliability Entity, INC.)
* IMM (Independent Market Monitor)
* VENDOR
* IMRE (Independent Market Information System Registered Entities)

The certificate type is based on the DUNS number provided in the application. The account type determines which role(s) the MP USA can assign within an entity. For additional information, refer to Section 1.4 MP USA Overview above.

Once an MP USA’s Digital Certificate is issued, email notifications are sent to the MP USA with instructions to download the certificate. Refer to the MPIM process defined in this guide.

* 1. **I am the USA, now what?**

The USA must evaluate the requirements for issuing Digital Certificates to meet the security needs of their entity. We recommend to create and maintain documentation to justify the need for a Digital Certificate. ***As an example***, ERCOT policy requires all USER’s requesting a Digital Certificate to complete two forms, an “ERCOT Digital Certificate Policy and Agreement Form” and a “Request Form.” The purpose of the first document is to ensure USER’s are held accountable for the security and use of their Digital Certificate. The Request Form justifies the need for a Digital Certificate.

* 1. **I received my certificate, now what do I do?**

The USA should establish internal policies and procedures for managing certificates, including the USA Digital Certificate. The USA should keep a record of all certificates issued within his/her entity.

**\*\*IMPORTANT:** The USA Digital Certificate should not be shared between different USER’s. If a secondary USA certificate is required, then submit an NCI (Notice of Change of Information) form to establish a secondary USA. The NCI form can be located at <http://www.ercot.com/services/rq/>

***\*\* NOTE:*** *Each certificate has a one-year lifespan. This means the certificate must be renewed by the anniversary of its issuance to remain valid.*

The USA should also determine the best way to document the EDC issues. EDC documentation will aid the USA in any troubleshooting and expedite any help that comes from ERCOT. An Excel spreadsheet containing the important USER information is a good way to do this. The spreadsheet below is an example of the information necessary to the USA.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **DUNs** | **First Name** | **Last Name** | **Employee ID** | **Email Address** | **Roles** | **Cert. State** | **Cert. Exp. Date** |
| 11111 | John | Doe | 1234 | name@XXX.com | XYZ | Valid | 6/10/2013 |
| 11111 | Mary | Jane | 1234 | name@XXX.com | XYZ | Expired | 7/7/2010 |

* 1. **Distribution for End USER’s**

USER EDCs authorized by the USA through the MPIM system are distributed to the end USER directly via email notifications from the system. See “Certificate Management” later in this guide for details.

* 1. **Backing up for Unplanned Issues**

The USA should define and support a back-up process to minimize the possibility of being without access to the ERCOT systems. The USA is the single point of entry for all EDCs issued by ERCOT; he/she should ensure that a back-up plan is established.

* 1. **Test Certificates**

Request for a TEST EDC to access the Market Operating Testing Environment (MOTE) are to be made through your ERCOT Account Manager or by sending an email to [ClientRelations@ercot.com](mailto:ClientRelations@ercot.com). For questions regarding a MOTE EDC, please contact your ERCOT Account Manager.

The MOTE URL is: <https://testmis.ercot.com/>

* 1. **API/Software Certificates**

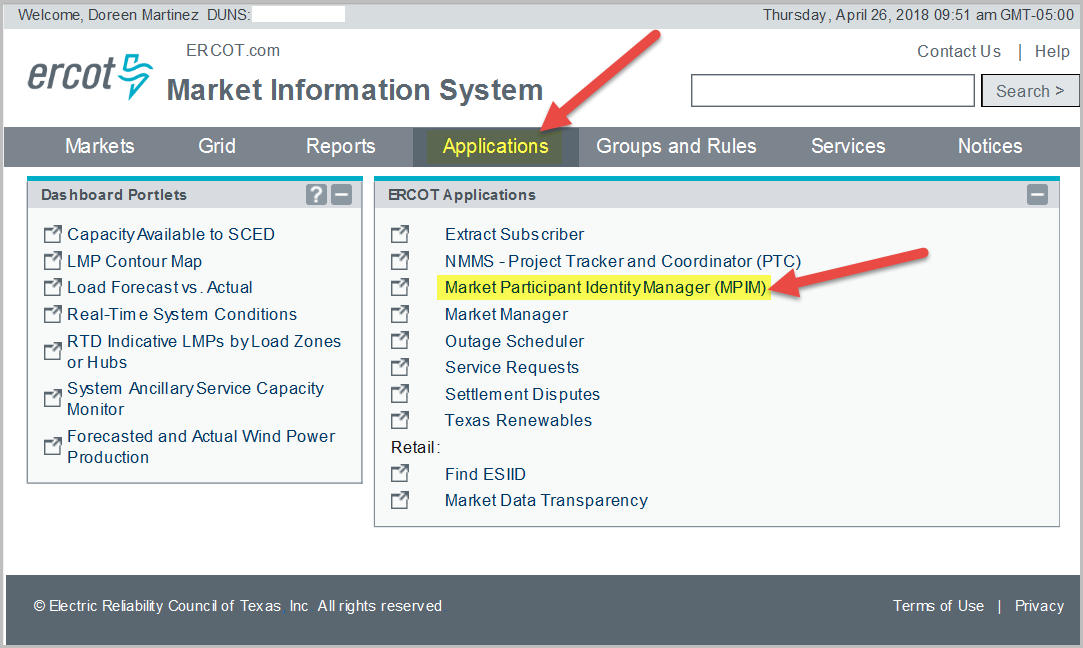
API and software Digital Certificates are enrolled in a similar manner to regular USER’s. However, the naming conventions for API/Software EDCs are different from the convention used for individuals. Please refer to the “Naming Convention” section of this guide for further information.

1. **Market Participant Identity Management Functionality**
   1. **Assumptions**
2. The MP has been qualified according to ERCOT’s registration process.
3. MP USA has a valid EDC for their organization.
   1. **Accessing MPIM**
4. Navigate to the Market Information System (MIS) Portal by inserting the following URL in a browser window: <https://mis.ercot.com/pps/tibco/mis>
5. Once prompted, select a certificate corresponding to the entity you are managing, by highlighting the MP USA certificate and click “**OK**” to continue. See examples below:

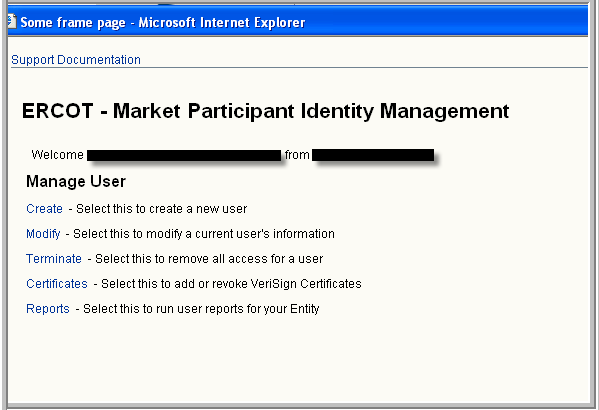


***The ERCOT Market Information System (MIS) Portal will load.***

1. Click on the **Applications** link located at the top of the MIS home page, and then click on the **Market Participant Identity Manager (MPIM).**



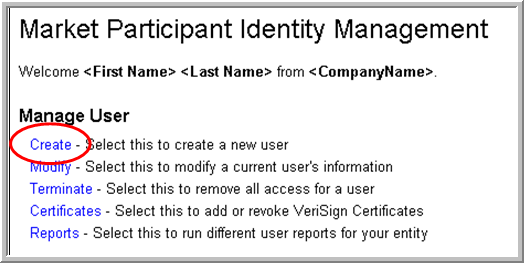
1. The MP USA will be presented with the MIS/MPIM screen shown below.



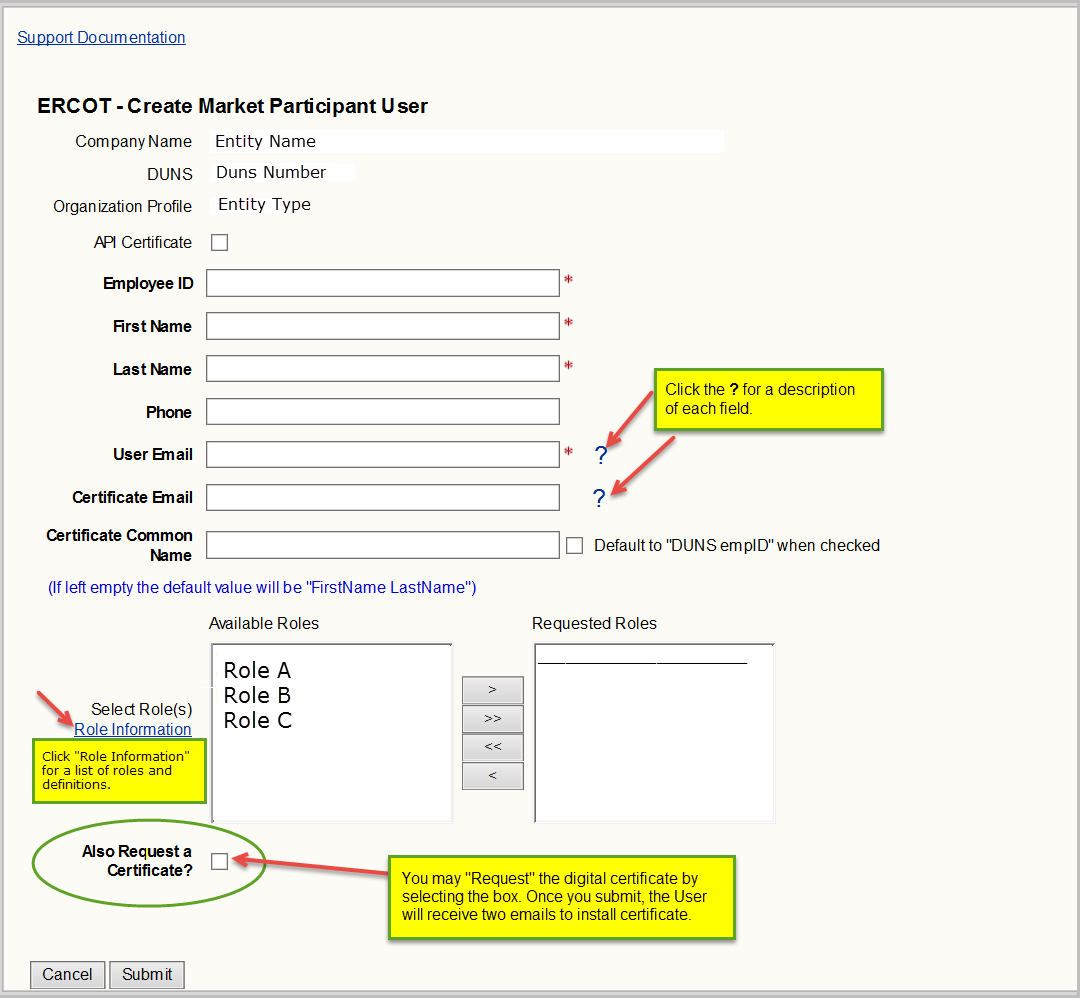
* 1. **Create MPIM USER Account**

To create a USER account within the MPIM system, the MP USA must be at the MPIM home page shown below.

1. MP USA clicks on the Create link.



MPIM presents the **Create Market Participant USER** page. The following information is pre-populated: Company Name, DUNS Number and Organization Profile.



**\*\* NOTE**:

* The Role Information link will direct you to the “Digital Certificate Security Information” page on ercot.com, click on “MPIM Digital Certificate Roles” to see available roles and definitions.
* Roles will vary per entity type.

*The following table shows the character limits and rules of allowable entries.*

|  |  |  |
| --- | --- | --- |
| Field Name | Length/Type | Validation |
| Employee ID | 4/min  19/max  Alpha-Numeric | * Unique within the MP entity * Should not contain any symbols * Should not contain any spaces * Should not contain any special characters |
| First Name | 30/Alpha-numeric | Should not contain any symbols or any special characters |
| Last Name | 30/Alpha-numeric | Should not contain any symbols or any special characters |
| Email | 100/Alpha-numeric | Must contain a “@” and “.’ |
| Common Name | 48/max Alpha-Numeric | Should not contain any symbols or any special characters |

1. MP USA fills out the required fields and assigns suitable roles. For more information regarding roles, click on the “Role Information” link.

To modify roles after the USER EDC has been created; select “Modify” on the MPIM home page, search for USER, update roles and submit.(**It is not necessary to revoke and reissue the Digital Certificate)**

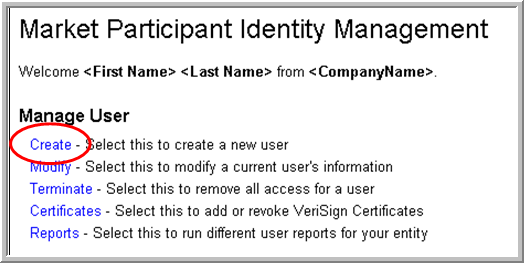
**\*\* NOTE**: If the EDC is not retrieved in five days, then the password will expire and the USER must contact the MP USA for reissuance*.*

**\*\*See Section 5 for assignment of roles for NMMS, EMS MOTE and SOTE.**

* 1. **Create Application Programming Interface (API) MPIM Account**

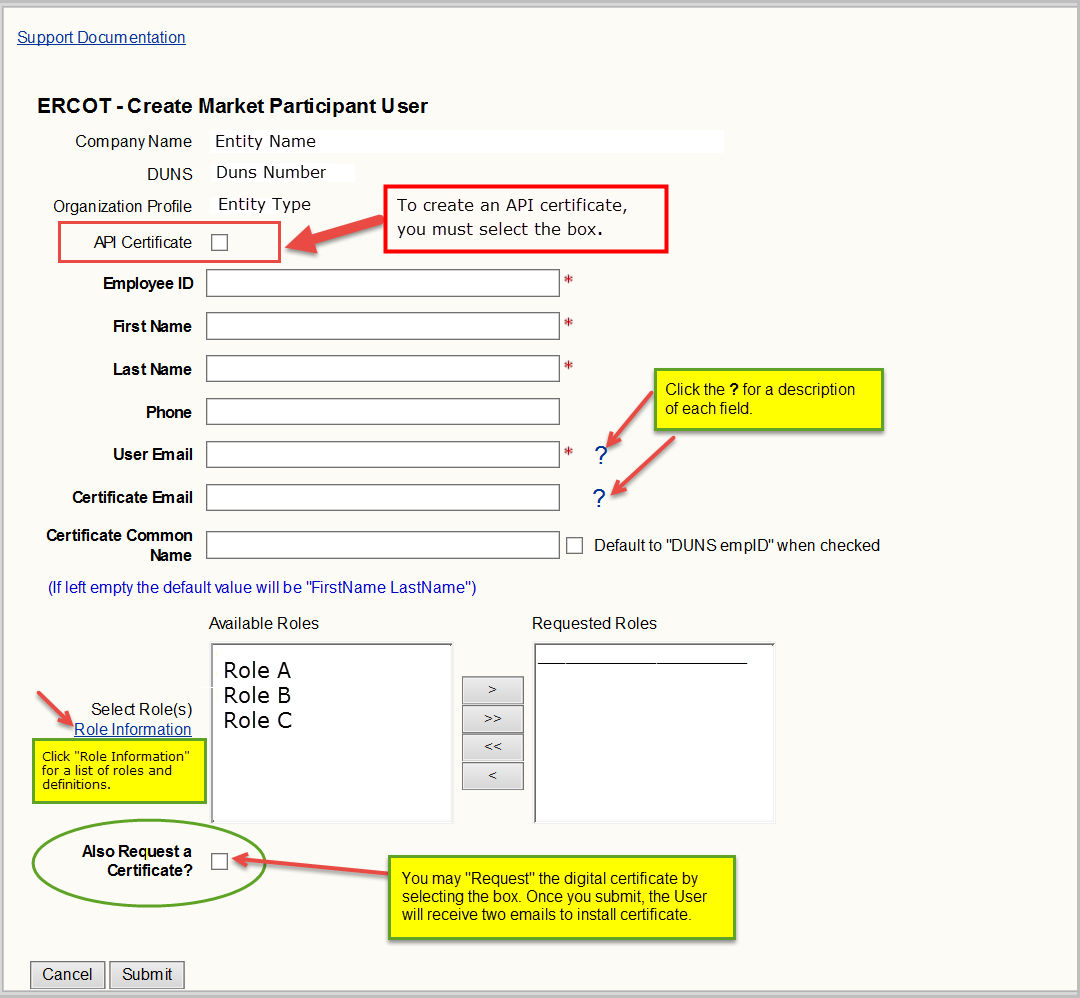
To create an API account within the MPIM system, the MP USA must be at the MPIM homepage (shown below).

1. MP USA clicks on the Create link.



MPIM presents the **Create Market Participant USER** page. The following information is pre-populated: Company Name, DUNS Number and Organization Profile.

1. MP USA must check the **“API”** box, populate the required fields, assign roles and then click on the “Submit” button.



*The following table shows the character limits and rules of allowable entries.*

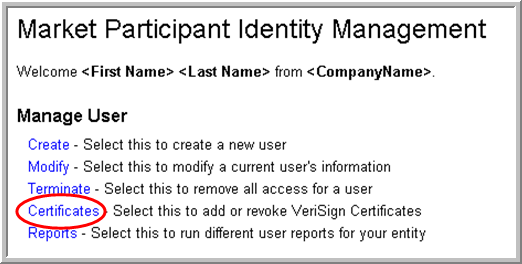
|  |  |  |
| --- | --- | --- |
| Field Name | Length/Type | Validation |
| Employee ID | 4/min  19/max  Alpha-Numeric | * Unique within the MP entity * Should not contain any symbols * Should not contain any spaces * Should not contain any special characters |
| First Name | 30/Alpha-numeric | Should not contain any symbols or any special characters |
| Last Name | 30/Alpha-numeric | Should not contain any symbols or any special characters |
| Email | 100/Alpha-numeric | Must contain a “@” and “.’ |
| Common Name | 48/max Alpha-Numeric | Should not contain any symbols or any special characters |

The MP USA is returned to the **Market Participant Identity Management** screen.

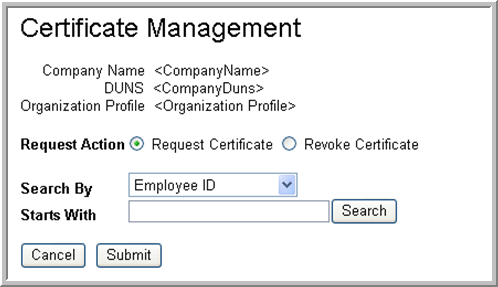
* 1. **Certificate Management**
     1. **Issue/Reissue USER Certificate in MPIM**

In order to request a USER certificate within the MPIM system, the MP USA must be at the MPIM home page (shown below).

1. MP USA selects the Certificates link.

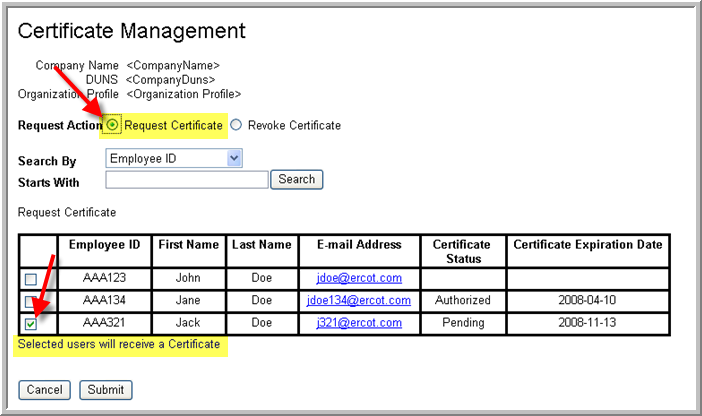


MPIM presents the **Certificate Management** page. The following information is pre-populated: Company Name, DUNS Number and Organization Profile. The “Request Certificate” radio button is pre-selected*.*

**

1. MP USA enters search parameters for a USER (employee id, first name, or last name).
2. MP USA clicks the “Search” button to retrieve USER information.

MPIM returns the search results in table format.



1. MP USA checks the USER(s) for whom EDCs should be generated, if not yet requested on the create page.
2. MP USA clicks the “Submit” button.

The MP USA is returned to the **Market Participant Identity Management** home page**.**

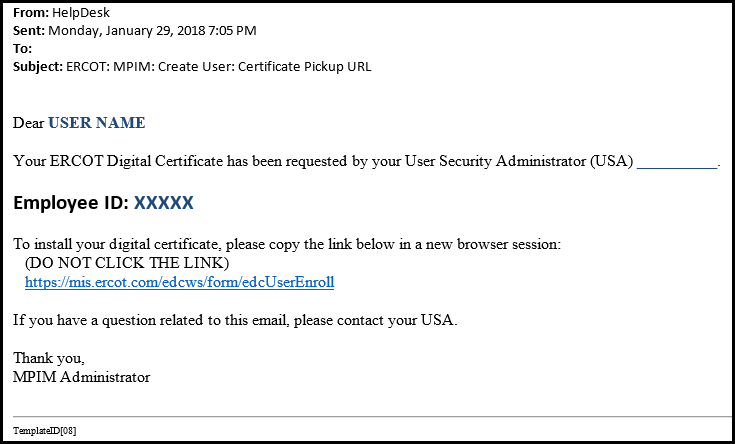
The selected USER(s) will receive two emails to retrieve their ERCOT Digital Certificate.

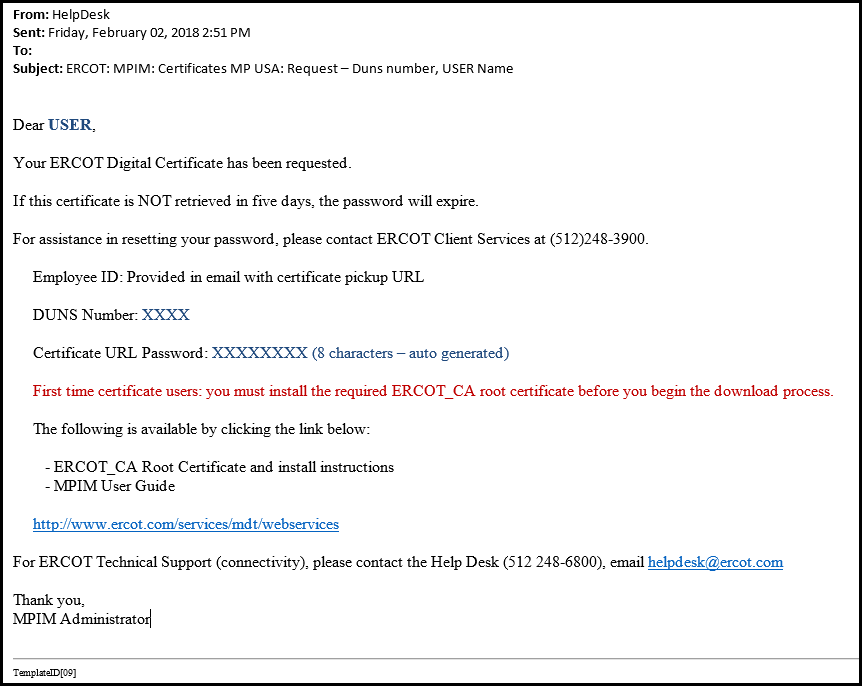
* + 1. **USER Certificate Retrieval**

This section assumes the MP USA has completed the steps defined in Section 4.5.1 and expands on the information in step 5 of the EDC request process.

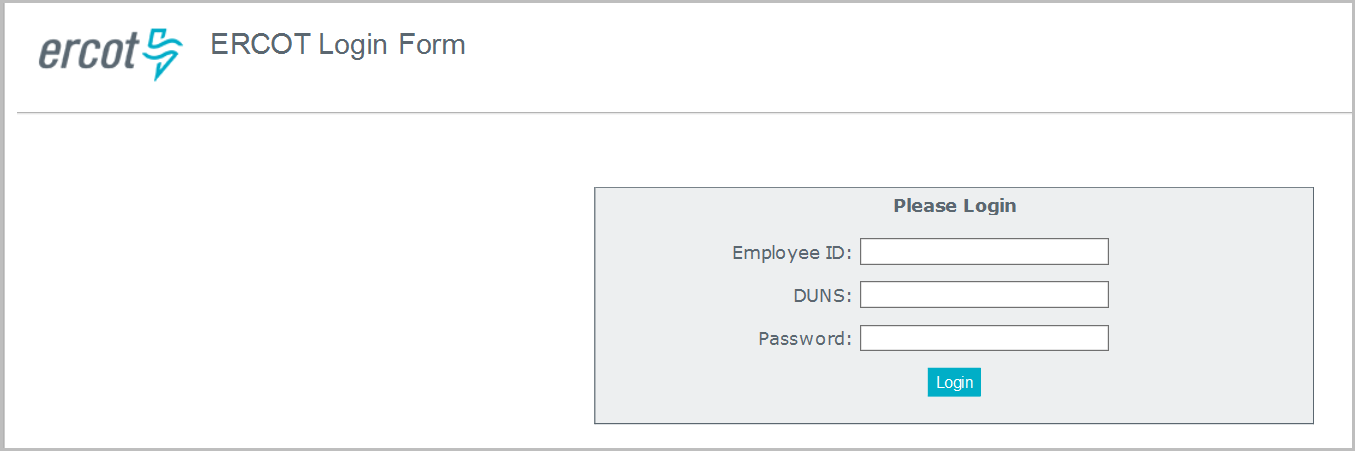
**\*\* NOTE**: If the EDC is not retrieved in five days, then the password will expire and the USER must contact the MP USA for reissuance*.*

1. Once the “Requested Certificate” is issued, the USER will receive two emails which are required to begin the installation process of their EDC. One email will contain the Employee id, DUNS number and Certificate Pickup URL and the other will provide the PASSWORD and the DUNS number. For security reasons, the password is only valid for one attempt. If the installation fails, the USA must reissue the USER EDC.

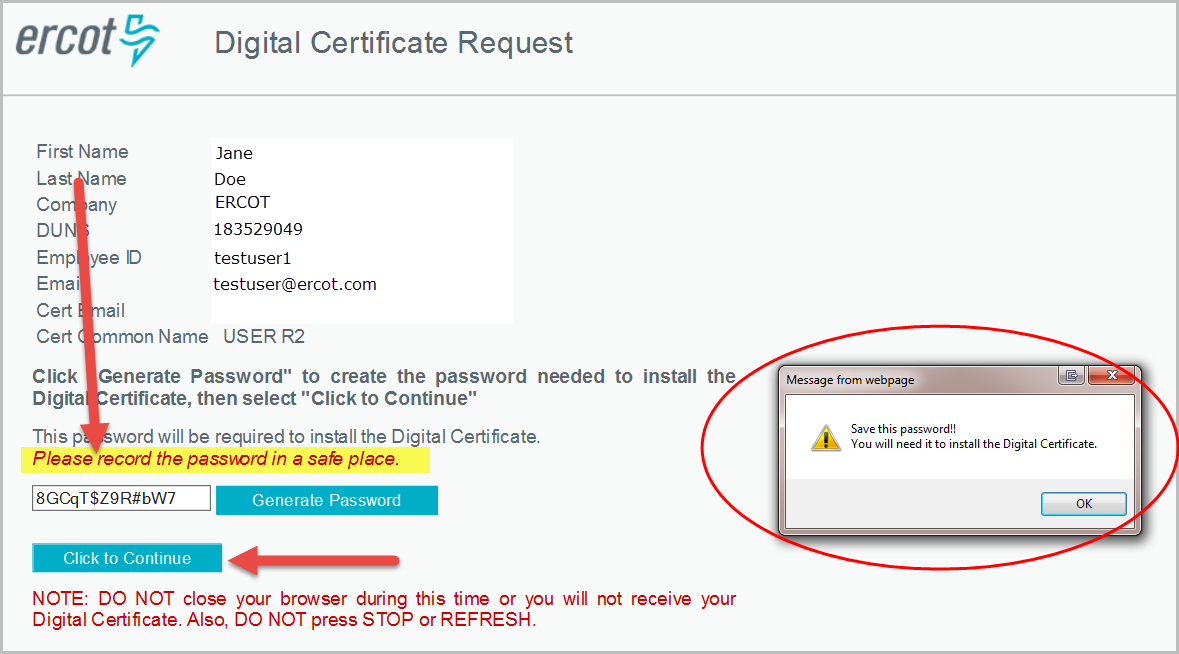




1. To download the certificate, the USER must copy and paste the certificate URL link into a “NEW” browser. The following login form will appear.



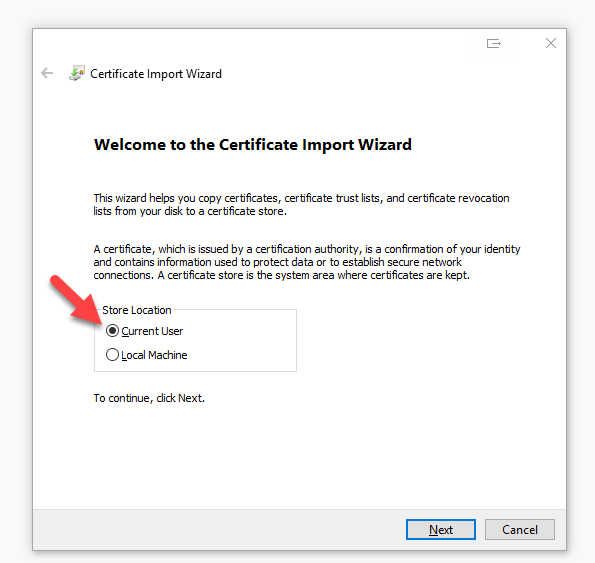
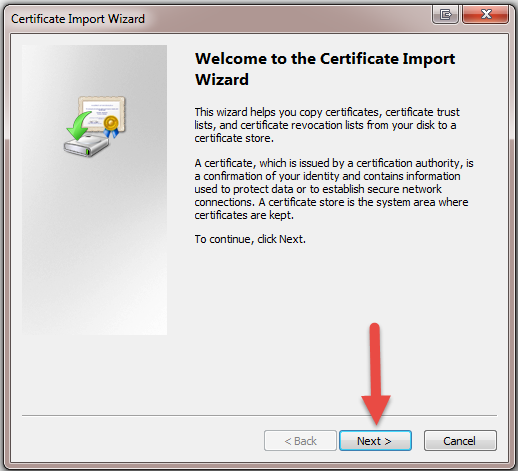
1. The USER is required to enter an Employee ID, DUNS Number and Password. The password is provided via email (see step 1 of this section). The random generated password must be eight (8) characters.
2. The USER will select “**Login**” to begin the downloading process.
3. The EDC site will authenticate the credentials and prompt the USER to accept the website and the USER will click the “**Yes**” button to continue.
4. The USER should verify their information, click “Generate Password” and then select “OK” to acknowledge the “Save this password” pop-up message.
5. **Copy or write down** the randomly generated password and click “Click to Continue”.



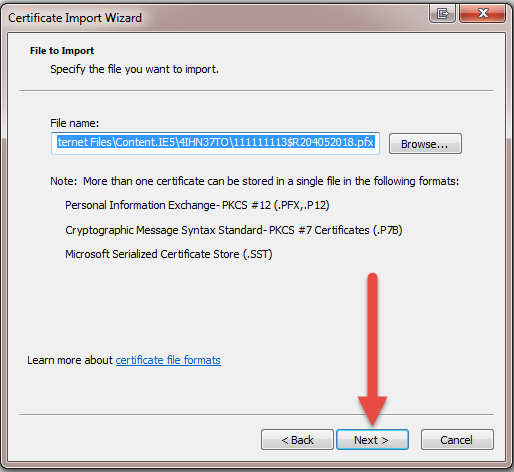
1. You now have the option to either “Open” the certificate to begin the installation process, or “Save” the certificate to your machine.



1. In the example, the “Open” button was selected to begin the installation process. The Save option will be discussed in Step 17.
2. Select “Current User”, Next and click Next again on the Certificate Import Wizard

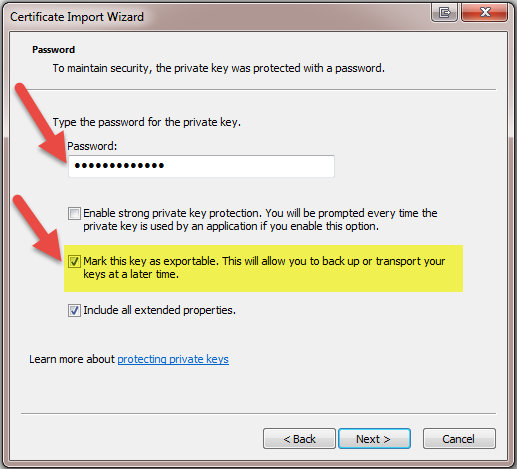
 

1. Click Next on the “File to Import” screen.



1. Type the randomly generated password created in Step 6 and check the “Mark this file as

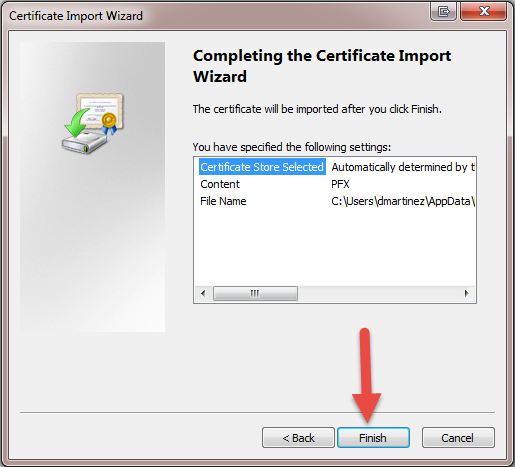
Exportable”, Click Next.



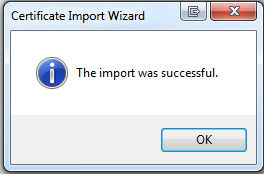
1. Click Next on the “Certificate Store” screen.



1. Verify certificate information and click Finish.



1. Click OK to Exit the Wizard.



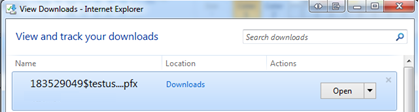
1. In this example, the “Save” button was selected to begin the installation process.



1. Click “View Downloads” under the Gear icon on the top right corner of the Internet Explorer browser.



1. Select the certificate that was downloaded and click Open.



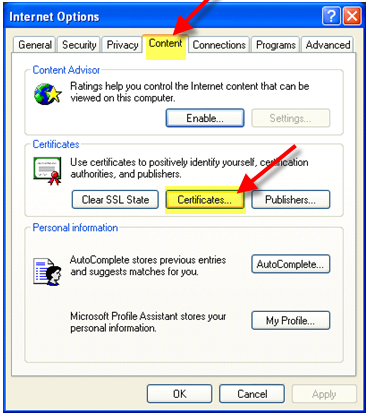
1. Follow steps 10-16 to complete the install.
   * 1. **Viewing Certificate Details**

To view details (Expiration Date, Name of Certificate, EID, and DUNS) of all the EDCs installed on a computer:

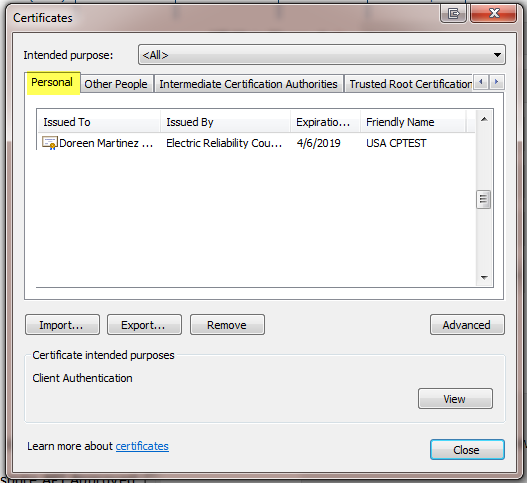
1.) Open Internet Explorer

2.) On the taskbar, go to Tools>>Internet Options

3.) In the window that pops up (shown below) click on the **Content tab** and then **Certificates**.

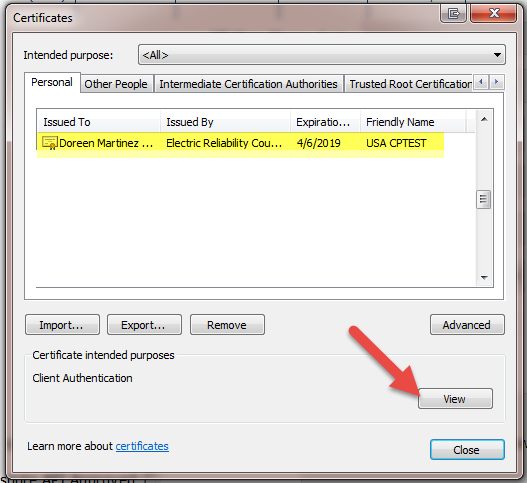


4.) The Certificates window will show all the EDCs installed on that computer.



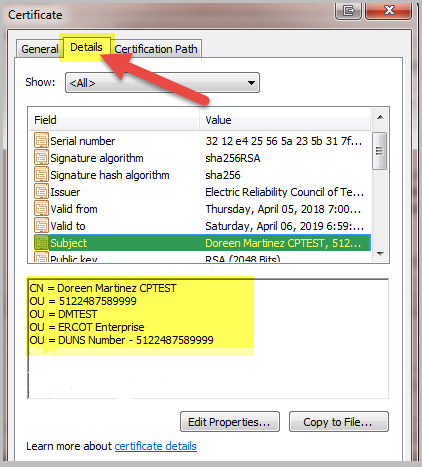
**\*\* NOTE: The expiration date is available in the Certificate window.**

5.) Highlight the EDC and click on “View” to see the details.



6.) Click on the “Details” tab within the next window (shown below).

7.) Highlight the subject line for certificate details.



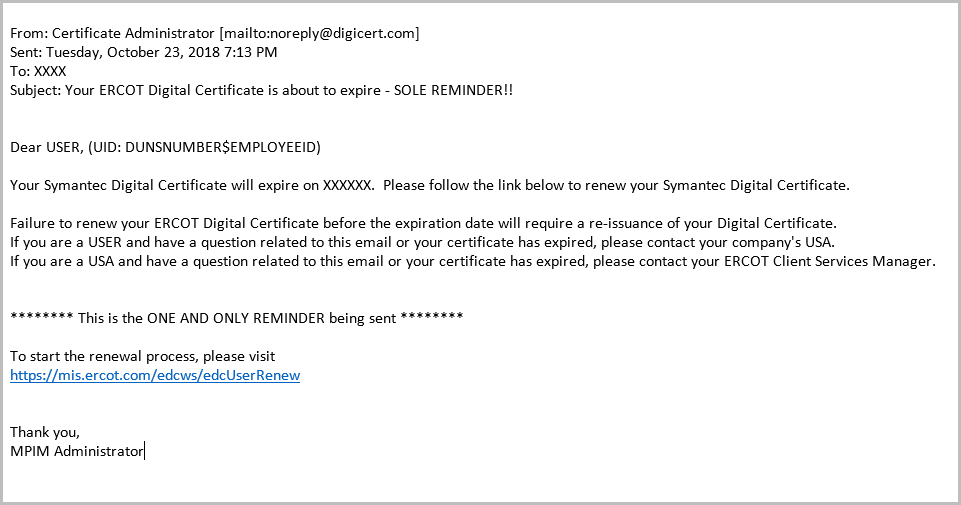
* + 1. **Lost or Corrupt Certificate**

In the event of a lost or corrupt MP USA certificate, please contact the ERCOT helpdesk at (512) 248-6800. Your duns number is required to open a helpdesk ticket. If a USER requires a new EDC, then he/she should contact their MP USA.

* + 1. **Certificate Renewal**

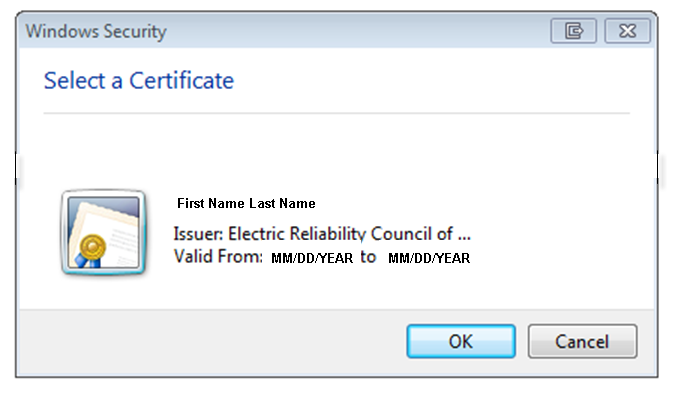
A renewal email is sent thirty (30) days prior to the expiration date of the Digital Certificate.

1. To renew the certificate, the USER will click on the link provided in the Certificate URL email (shown below).



**\*\* NOTE: Expired USER certificates are reissued by the MP USA. Expired USA certificates are reissued by the ERCOT USA.**

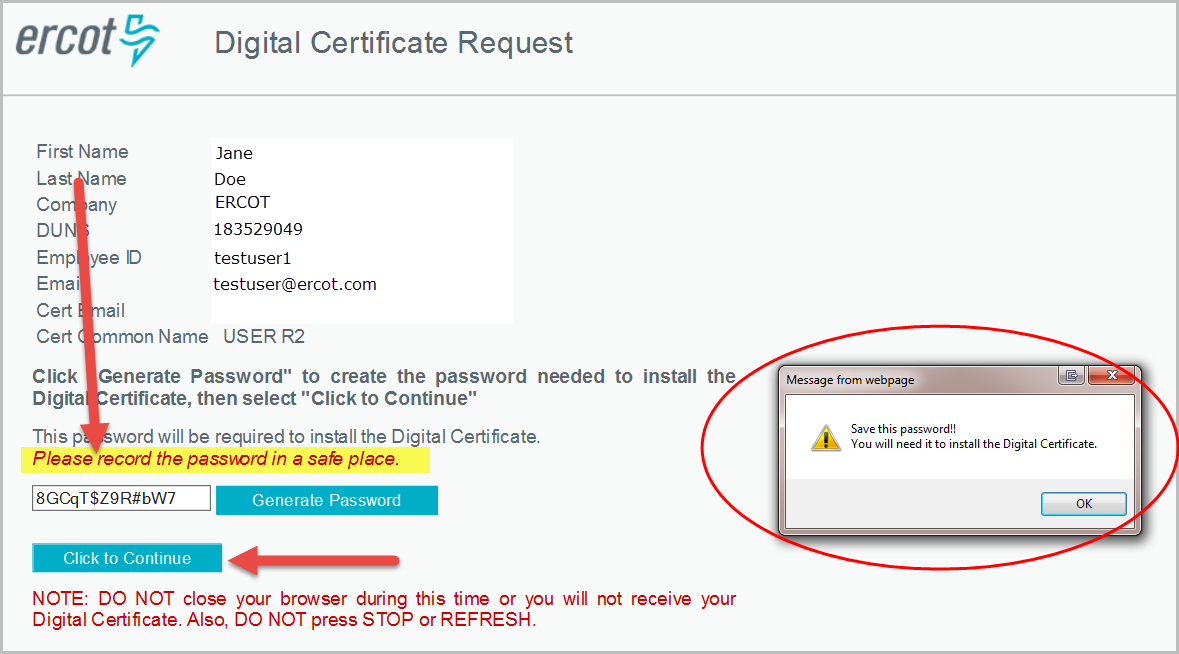
* + - 1. Select the Digital Certificate listed in the email and then click **OK**.



* + - 1. Check “Grant permission” and Click **OK**
      2. Younow have the option to either “Open” the certificate to begin the installation process, or “Save” the certificate to your machine



* + - 1. The USER should verify their information, click “Generate Password” and then select “OK” to acknowledge the “Save this password” pop-up message.
      2. **Copy** **or write down** the randomly generated password and click “Click to Continue”.

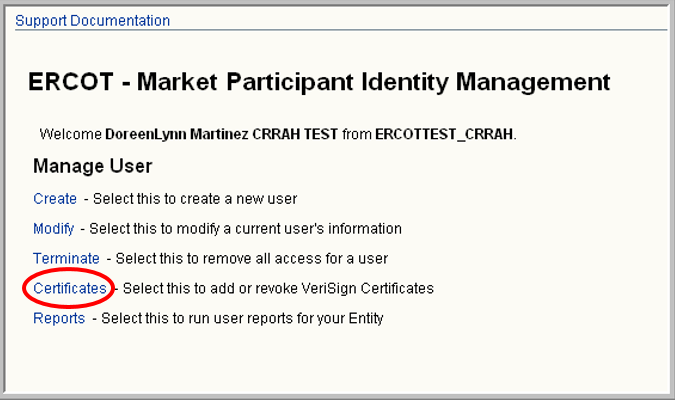


* + - 1. Follow the same install process as shown above in step 4.5.2.
    1. **Revoking USER Certificate in MPIM**

**\*\* NOTE:** Revoking the certificate does **not** terminate the USER’s MPIM account*.*

In order to revoke a USER EDC, the MP USA must be at the MPIM home page (shown below).

1. MP USA clicks on the Certificates link.

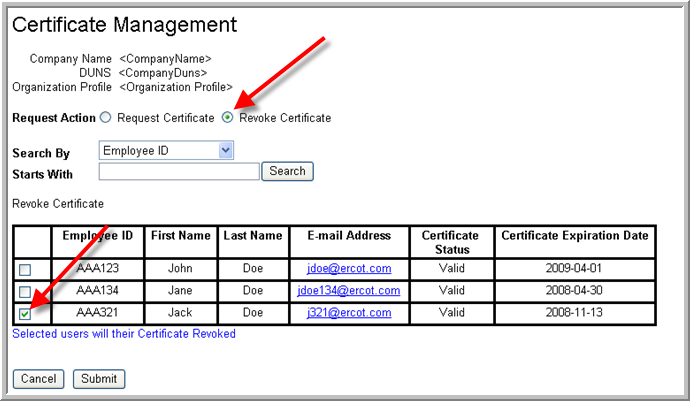


MPIM presents the **Certificate Management** page. The following information is pre-populated: Company Name, DUNS Number and Organization Profile.

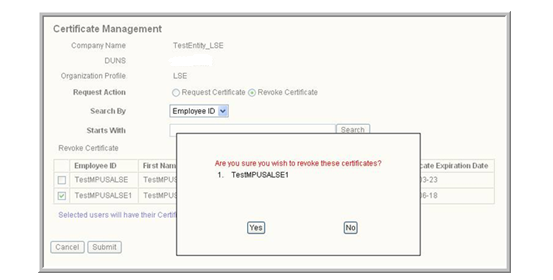


1. MP USA clicks the “Revoke Certificate” radio button.
2. MP USA enters the search parameters for a USER (employee id, first name, or last name).
3. MP USA clicks the “Search” button.

MPIM returns the search results in a table format.



1. MP USA checks the USER(s) for whom EDCs should be revoked.
2. MP USA clicks on the “**Submit**” button.
3. A confirmation box will appear with “Are you sure you wish to revoke these certificates?”
4. Select **Yes** or **No**.



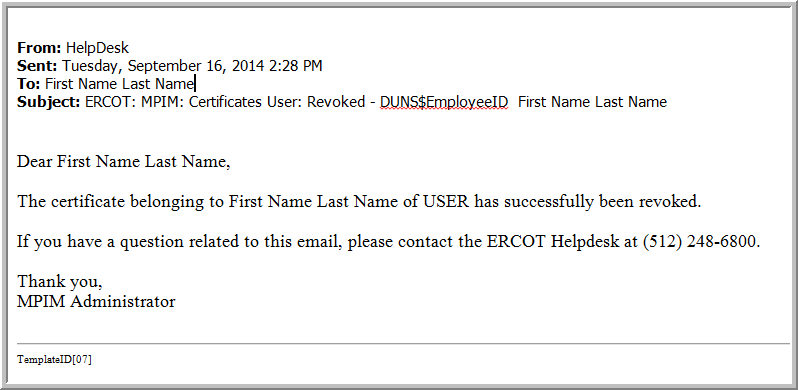
1. MPIM revokes the USER(s) EDCs.

The MP USA is returned to the **Market Participant Identity Management** screen.

1. Once the EDC revocation request is complete, the MP USA will receive the following email:

The MP USA is returned to the **Market Participant Identity Management** screen.

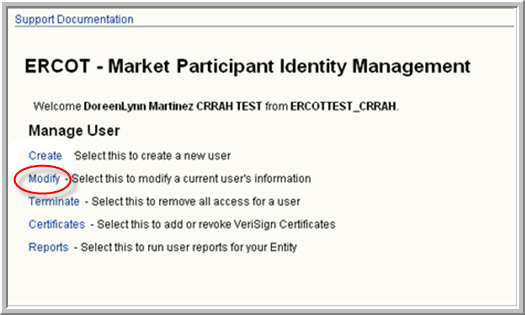
**Certificate Revoke Email:**



* 1. **Modifying a USER and API MPIM Account with Roles**

To modify a USER EDC in the MPIM system, the MP USA must be at the MPIM home page (shown below).

1. MP USA clicks on the Modify link.

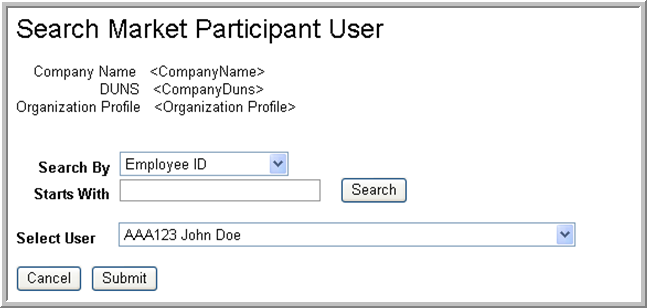


MPIM presents the **Modify Market Participant USER** page. The following information is pre-populated: Company Name, DUNS Number and Organization Profile.



1. MP USA enters search parameters for a USER (employee id, first name, or last name).
2. MP USA clicks the “**Search**” button.

MPIM generates the search results in a pull down menu.

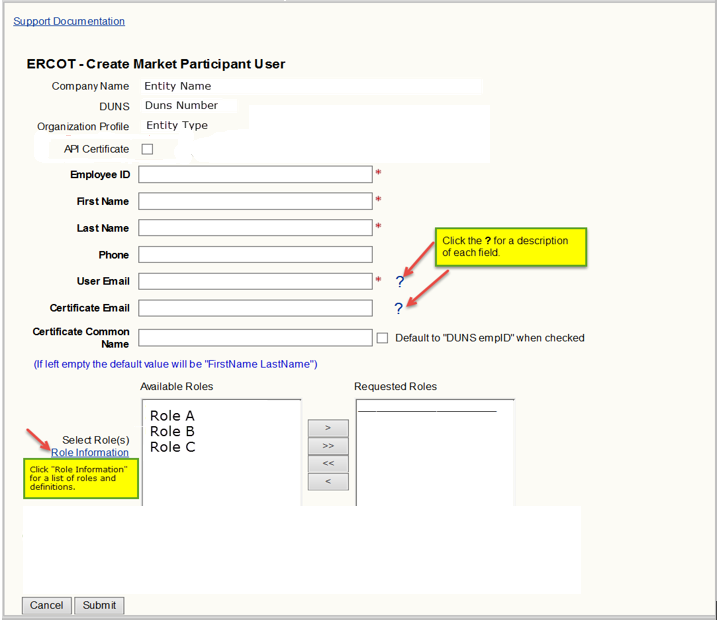


1. MP USA selects a USER.
2. MP USA clicks on the “**Submit**” button.

MPIM presents the **Modify Market Participant USER** page.

The following information is pre-populated: Company Name, DUNS Number and Organization Profile.

The USER information is also pre-populated since it’s an existing account.



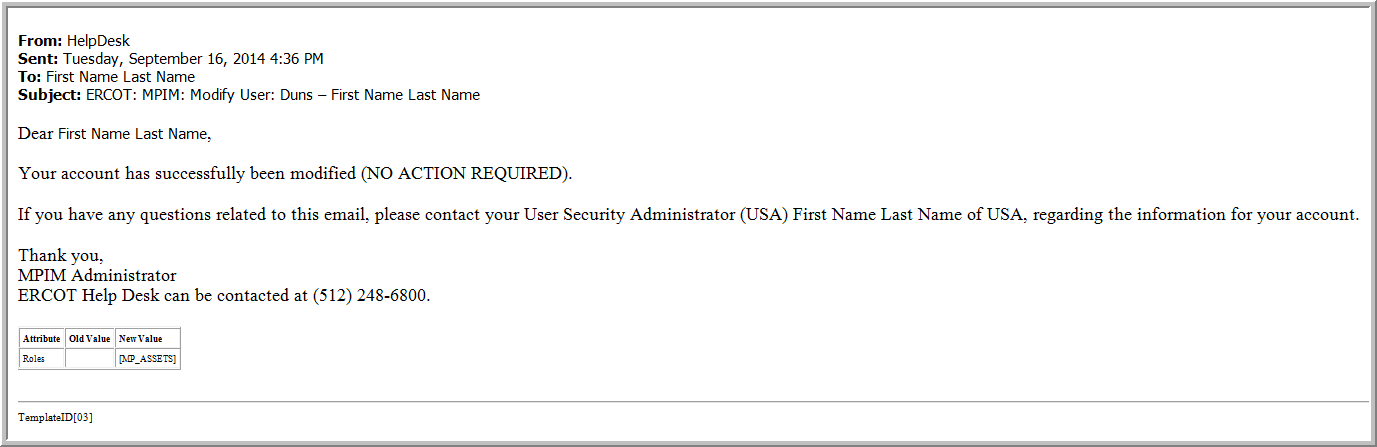
**\*\* NOTE**:

* The Role Information link will direct you to the “Digital Certificate Security Information” page on ercot.com, click on “MPIM Digital Certificate Roles” to see available roles and definitions.
* Roles will vary per entity type.

1. MP USA will modify required fields if needed.
2. MP USA modifies roles (**It is not necessary to revoke and reissue the Digital Certificate)**
3. MP USA clicks on the “**Submit**” button.

After the USER account is successfully modified, the following email is sent to the USER. The assignment of roles may also generate additional emails.

**Successful USER Account Modification email:**

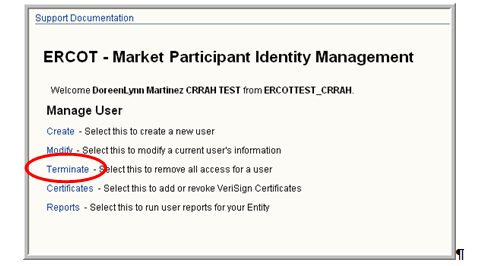


* 1. **Terminating a USER Account**

**\*\* NOTE:** Once a USER is terminated, you cannot reactive that account. If a USER EDC is inadvertently terminated, a new account (new employee id) must be created.

In order to terminate a USER account within the MPIM system, the MP USA must be at the MPIM home page.

1. MP USA clicks on the **Terminate** link.

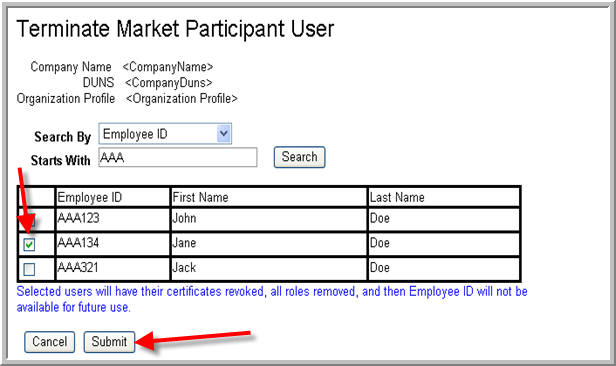


MPIM presents the **Terminate Market Participant USER** page. The following information is pre-populated:

Company Name, DUNS Number and Organization Profile.



1. MP USA enters search parameters for a USER (employee id, first name, or last name).
2. MP USA clicks the “**Search**” button. MPIM returns the search results in table format.



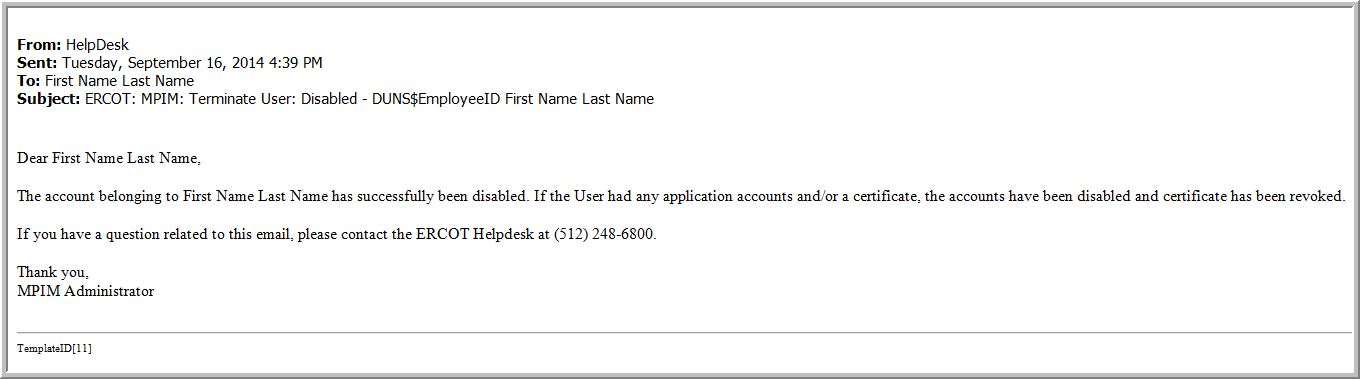
1. MP USA checks the USER(s) for whom EDC should be terminated
2. MP USA clicks on the “**Submit**” button.
3. A confirmation box will appear with “Are you sure you wish to terminate these USER’s?”
4. Select **Yes** or **No**.



The USER Certificate is terminated, roles are removed, and the account is disabled in MPIM.

MPIM sends a revoke notification email to the USER and a successful notification email to the MP USA. (Example of the email is below).

**USER Termination email:**



* 1. **Reporting**
     1. **Report Types and Data**

The MPIM makes the following reports available:

* Current Status Report (all active accounts for a DUNS)
* Full Report (entire history of all EDCs for a DUNS number)

The following information will be provided per USER in the Current Status and Full reports:

* First Name
* Last Name
* DUNS number
* Employee ID
* Email Address
* Cert Common Name
* Account State
* Roles Assigned
* Admin Role Assigned (This will be blank for most USER’s.)
* Certificate State
* Certificate Expiration Date
* NERC Certification Date (This field will not be populated.)

The MP USA can view the reports in the following formats: on screen (HTML), CSV (viewable in Excel) and a PDF document.

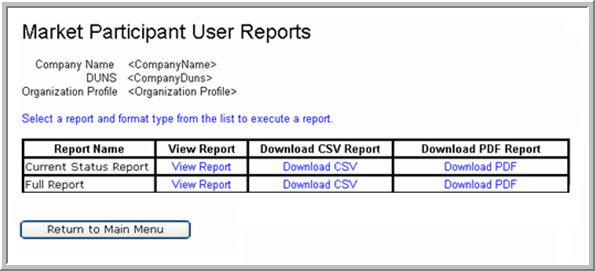
* + 1. **Downloading the report**

In order to view a report from the MPIM system, the MP USA must be at the MPIM home page shown below.

1. MP USA clicks on the **Reports** link.



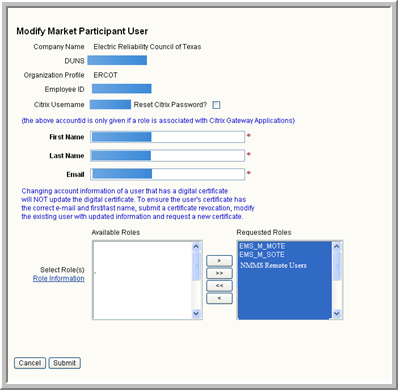
MPIM presents the **Market Participant USER Reports** page with the Company Name, DUNS Number and Organization Profile pre-populated.



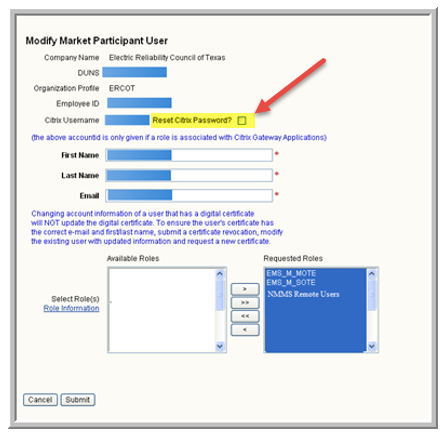
1. MP USA clicks the link for the desired Report Name:

* Current Status Report: Displays all valid certificates
* Full Report: Displays a history of all valid and terminated certificates

1. **TSP GATEWAY**
   1. **USA to assign the role for NMMS to remote USER’s**

****

* 1. **Reset Citrix Password (Go to Modify in MPIM)**

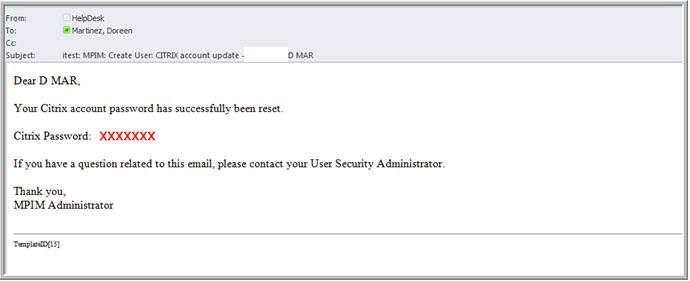


* 1. **Email Notification to USER**

The notification email below is sent to the USER. The new role is listed at the bottom of the email.



* 1. **Citrix Account Creation, Email and Password**

The Citrix account has been created and an email is sent with the Citrix Password (see below).

* 1. **Citrix Confirmation Email**

Once the Citrix account is created, the following email will be sent to confirm creation.



**Helpful Information for Citrix USER’s:**

**Windows 7**

1)      Install ‘Citrix Receiver” <http://receiver.citrix.com> . (It’s free.)

2)      No configuration of Receiver is required; you will use Citrix via the web browser. If the ERCOT Citrix Portals do not detect a version of receiver installed, you will be directed to <http://receiver.citrix.com> to install the appropriate version for your platform. When you click on a shortcut from the web interface you may be prompted to take an action for the .ICA file.  If so, simply click ‘Open’.

**Windows 8 and Windows 8RT**

Currently ERCOT does not support connecting directly through the Citrix Receiver client StoreFront features but it is still required to use Citrix.

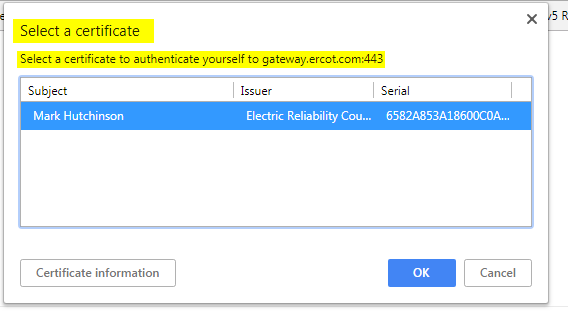
1)      Install ‘Citrix Receiver” from the Windows Store. (It’s free.)

2)      No configuration of Receiver is required; you will use Citrix via the web browser.  When you click on a shortcut from the web interface you may be prompted to take an action for the .ICA file.  If so, simply click ‘Open’.

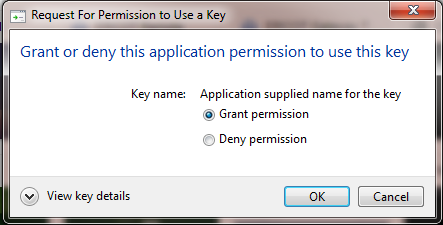
* 1. **Email to Administrator for USER Database Access**

An email is sent to the Administrator to create an individual USER account. This will grant USER access to the applicable Database.

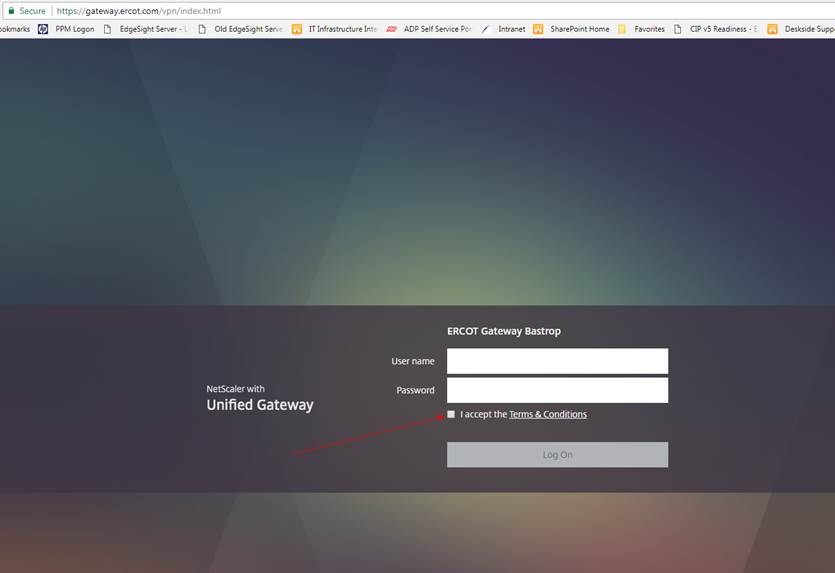
* EMS\_M\_MOTE
* EMS\_M\_SOTE
* NMMS\_REMOTE\_USER
  1. **Logging in to Citrix**
     + 1. **Before login, user may be prompted to accept/pick a certificate**



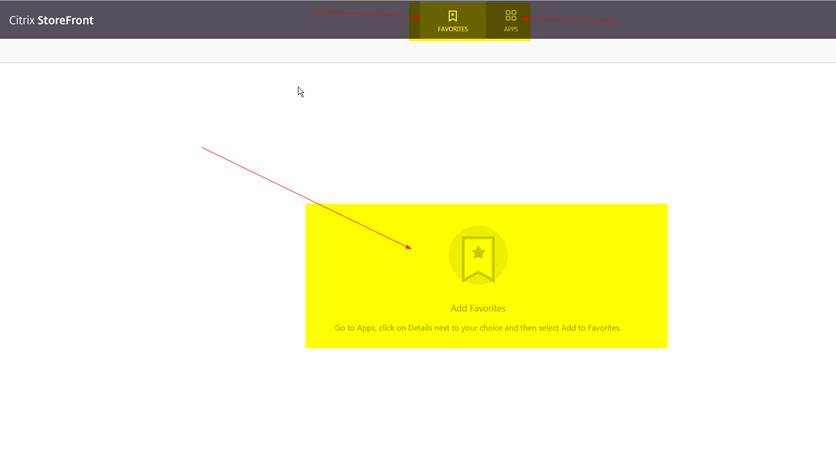
* + - 1. **Select grant permission to use the digital key**



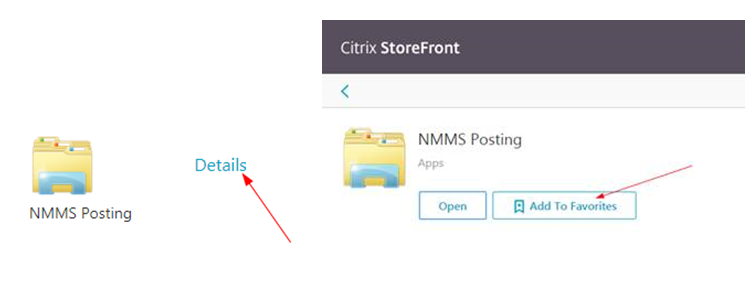
* + - 1. **The user must check the “I accept the Terms & Conditions” before the log on box is active.**



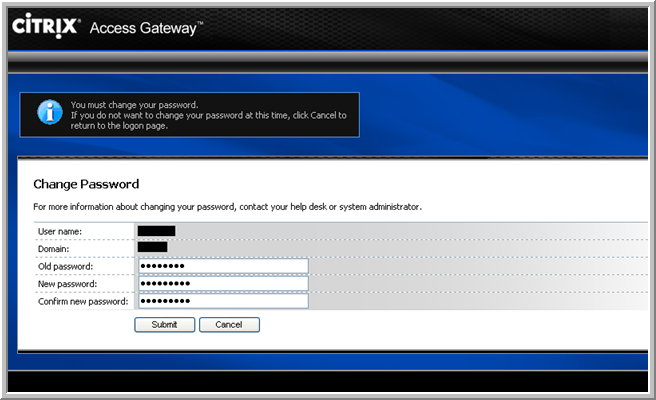
* + - 1. **Portal page will have two tabs at the top: Favorites and Apps – Favorites will be empty of applications the first time user logs in, click on the Apps Tab and select the applications you want added in your Favorites Tab – customizable per user.**



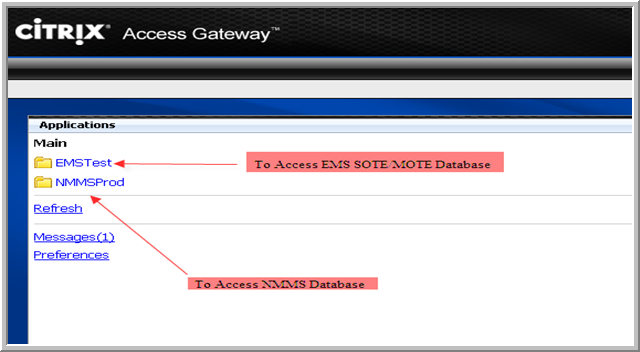
* + - 1. **To add applications to Favorites, first click on Apps Tab then find the application you want to add > then click on Details to the right of the application > then click ‘Add to Favorites’**



**5.8. USER is required to change password.**

****

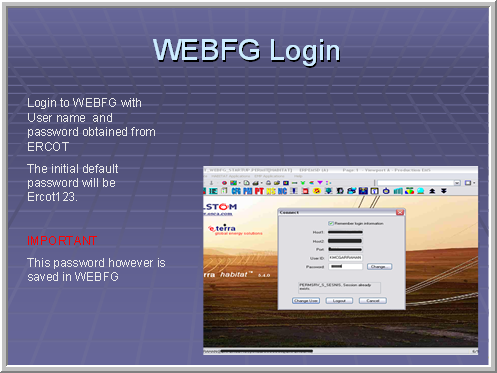
* 1. **Access to NMMS and EMS SOTE/MOTE Database**

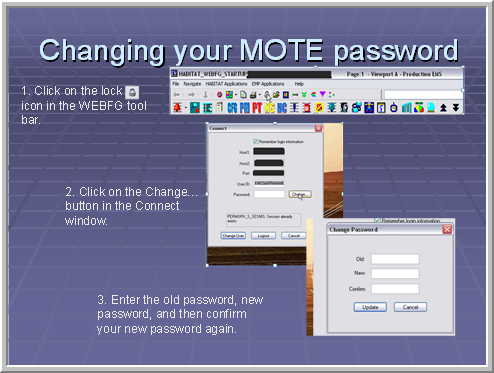


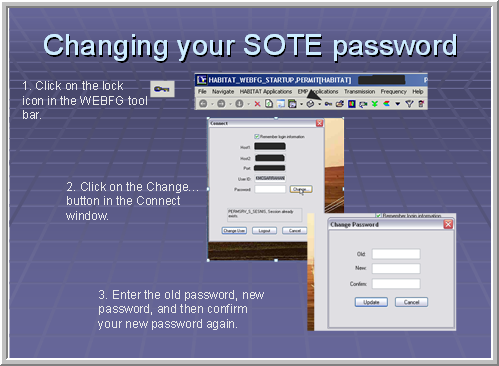
**\*\*\*** Note: USER’s will NOT be able to login to the NMMS production system until they have received an email from the NMMS team stating that their access has been granted.

**5.10 Login Procedures to WEBFG**

Once you have your Citrix account and password, you may login to WEBFG. See the login procedures listed below:

****





**Supporting Reference Documents**

The referenced documentation, Protocol Section 16.12 and the NCI form can be found at:

Protocol reference 16.12 USER Security Administrator and Digital Certificates:

<http://www.ercot.com/mktrules/nprotocols/current>

**NCI (Notice of Change of Information)**: This form is used by market participants to update, amend or correct information previously submitted to ERCOT: <http://www.ercot.com/services/rq>

MIS Roles: See section 4.3 or contact your ERCOT Account Manager to obtain a copy of the MIS role definitions and functions. **For updated documentation, contact your ERCOT Account Manager.**