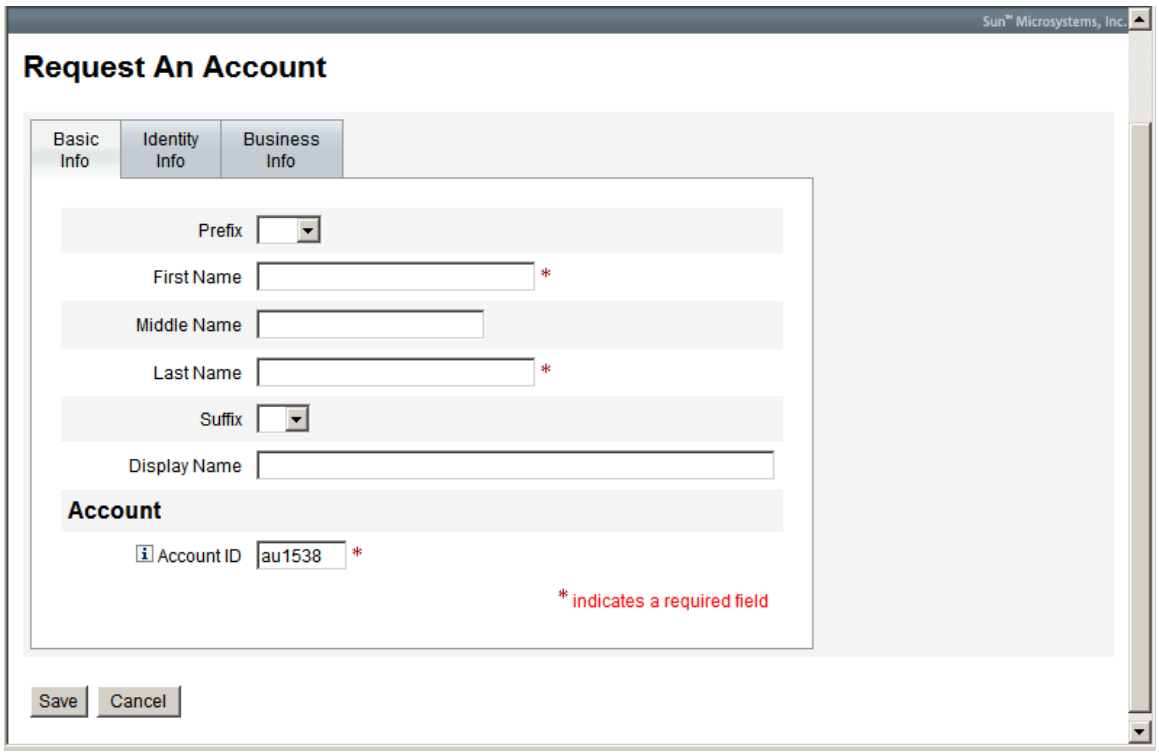
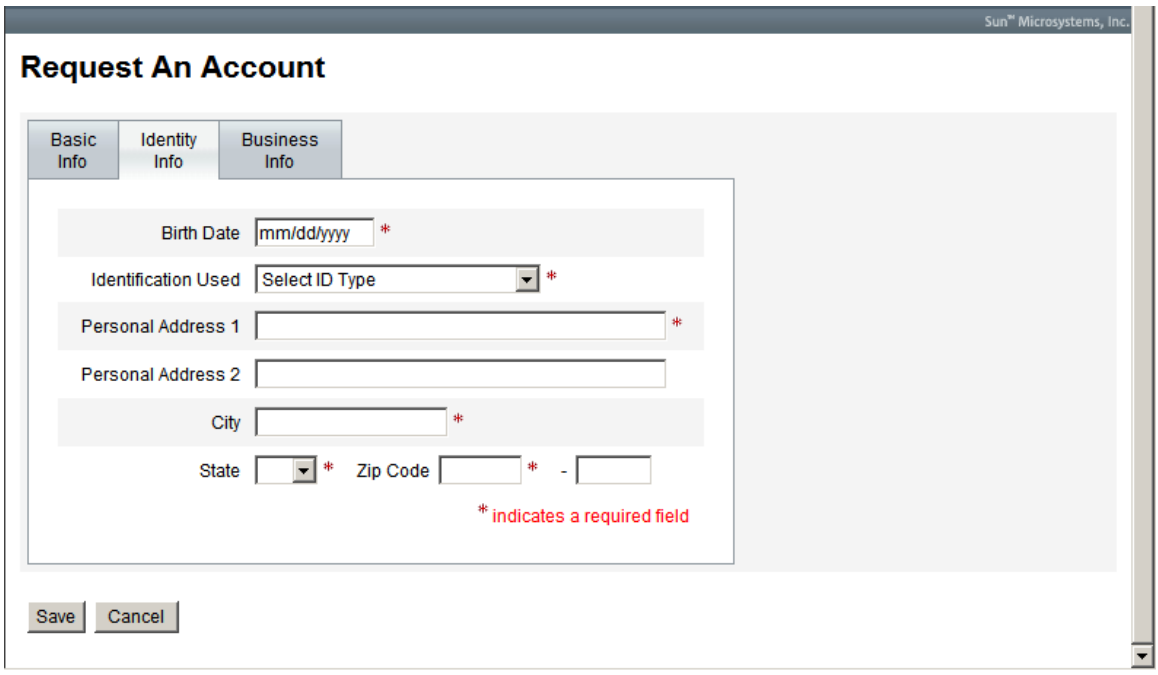
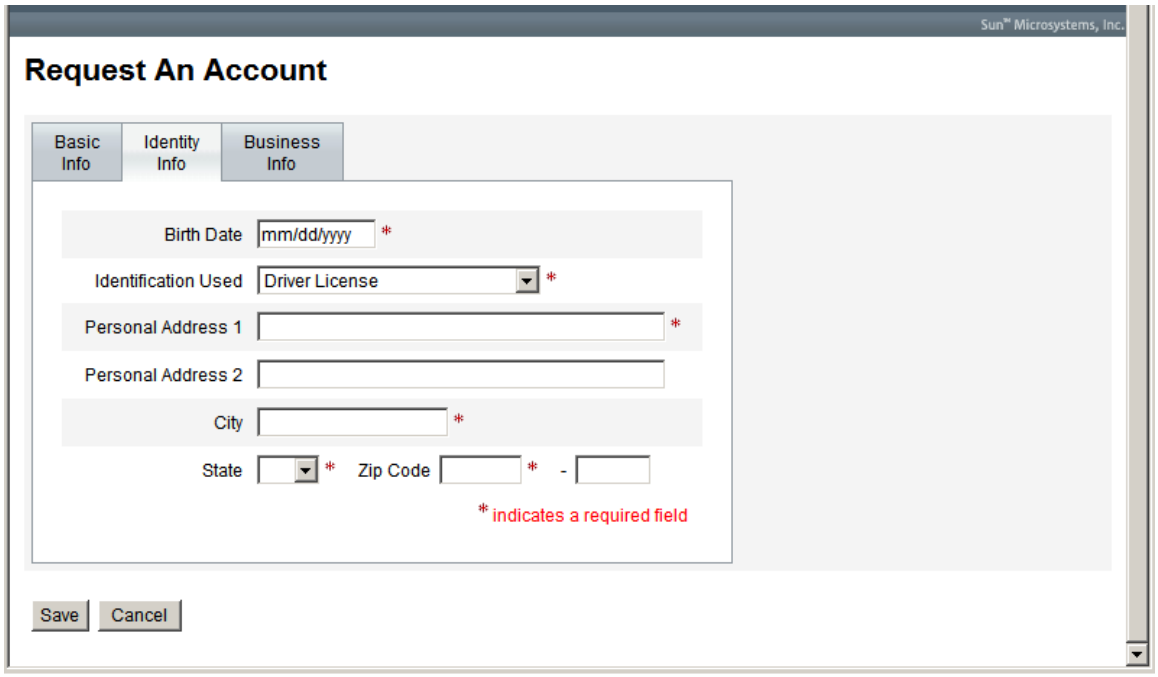
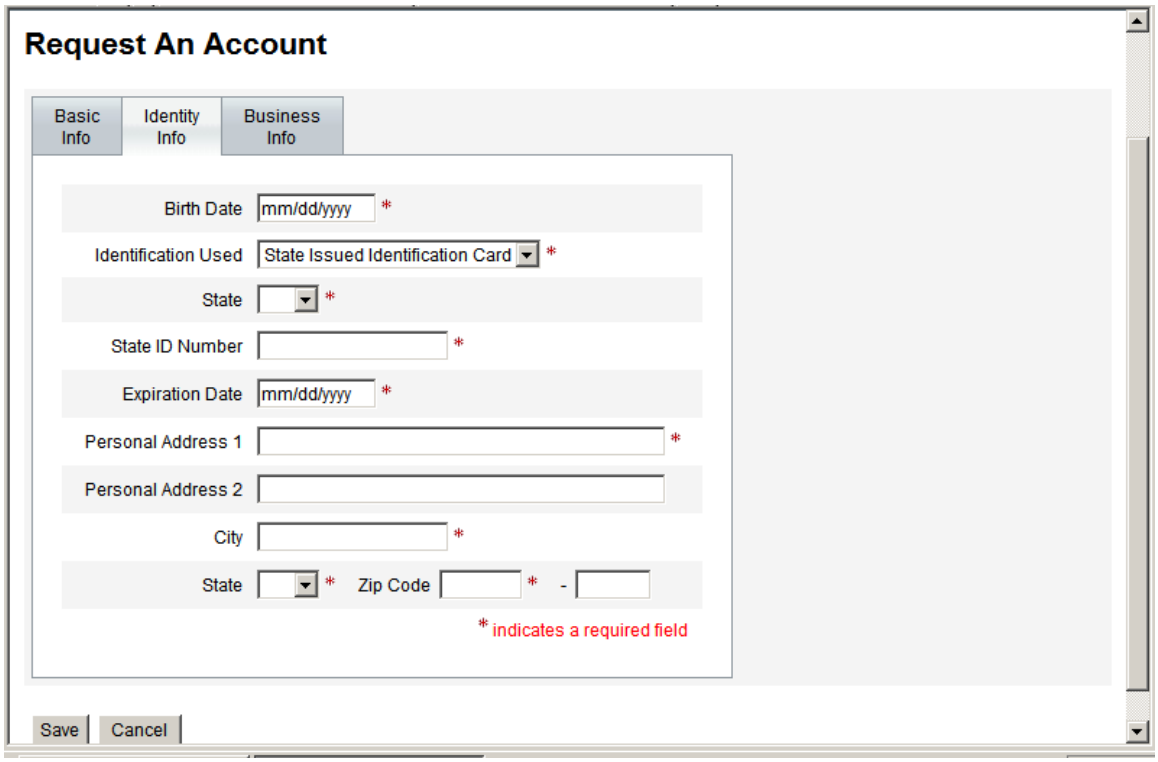
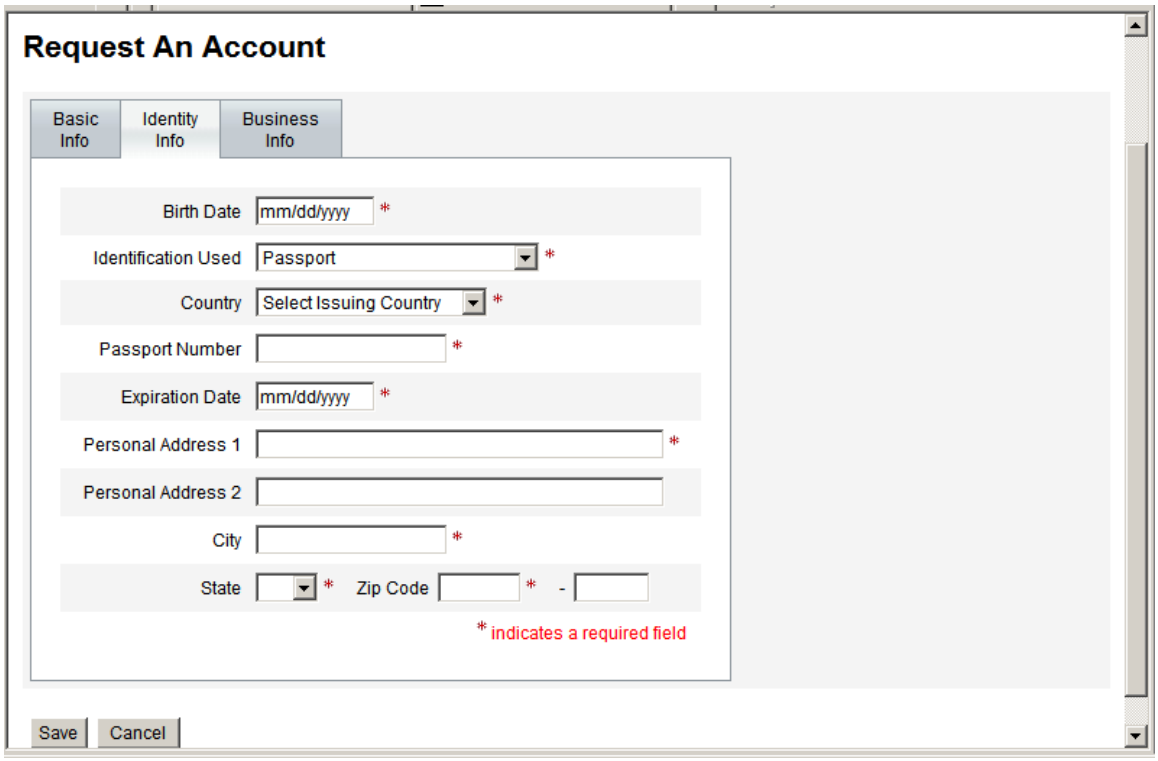
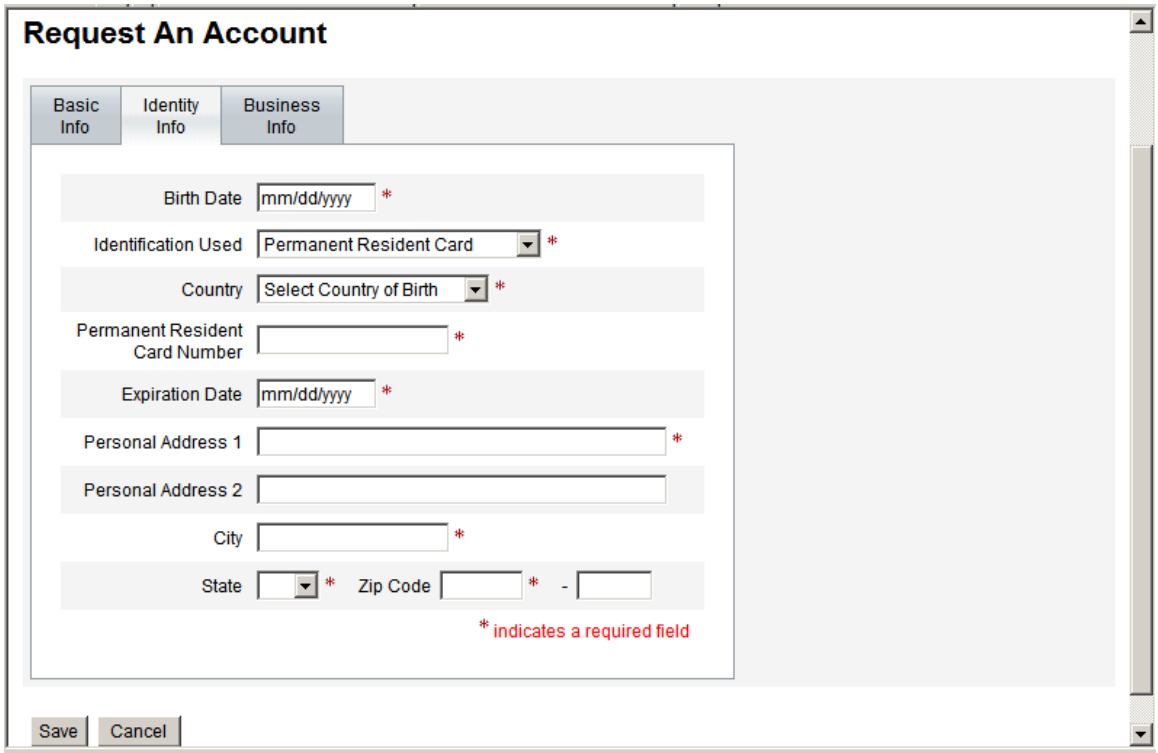

Sun™ Microsystems, Inc.
Request An Account
Basic Info
Identity Info
Business Info
Prefix
First Name
*
Middle Name
Last Name
*
Suffix
Display Name
Account
Account ID
au1538
*
* indicates a required field
Save
Cancel

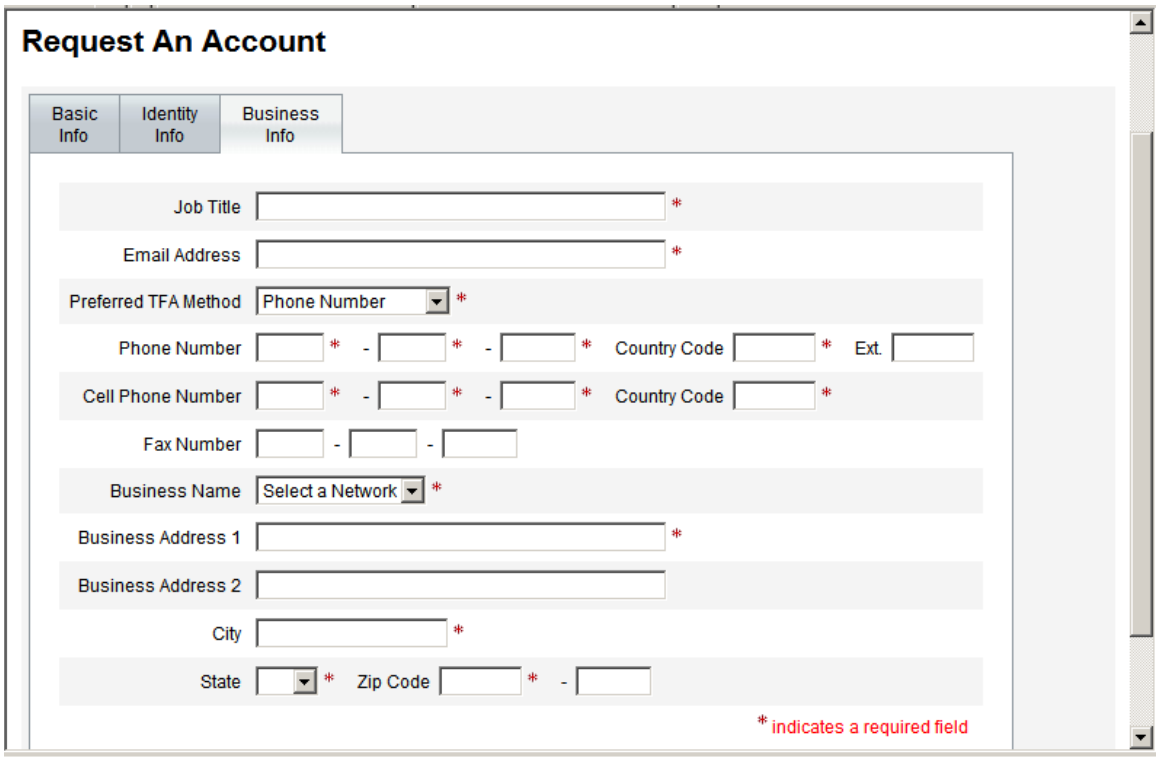

Sun™ Microsystems, Inc.
Request An Account
Basic Info
Identity Info
Business Info
Birth Date
mm/dd/yyyy
*
Identification Used
Select ID Type
*
Personal Address 1
*
Personal Address 2
City
*
State
*
Zip Code
*
-
* indicates a required field
Save
Cancel

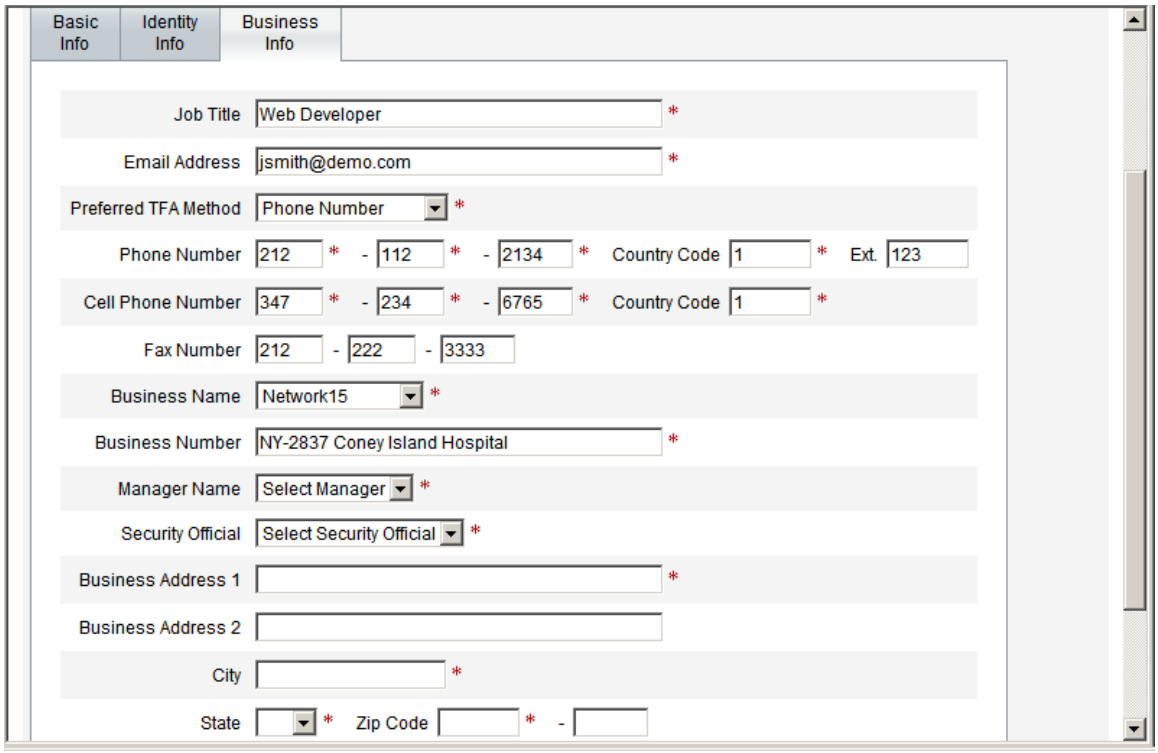

Sun™ Microsystems, Inc.
Request An Account
Basic Info
Identity Info
Business Info
Birth Date
mm/dd/yyyy
*
Identification Used
Driver License
*
Personal Address 1
*
Personal Address 2
City
*
State
*
Zip Code
*
-
* indicates a required field
Save
Cancel

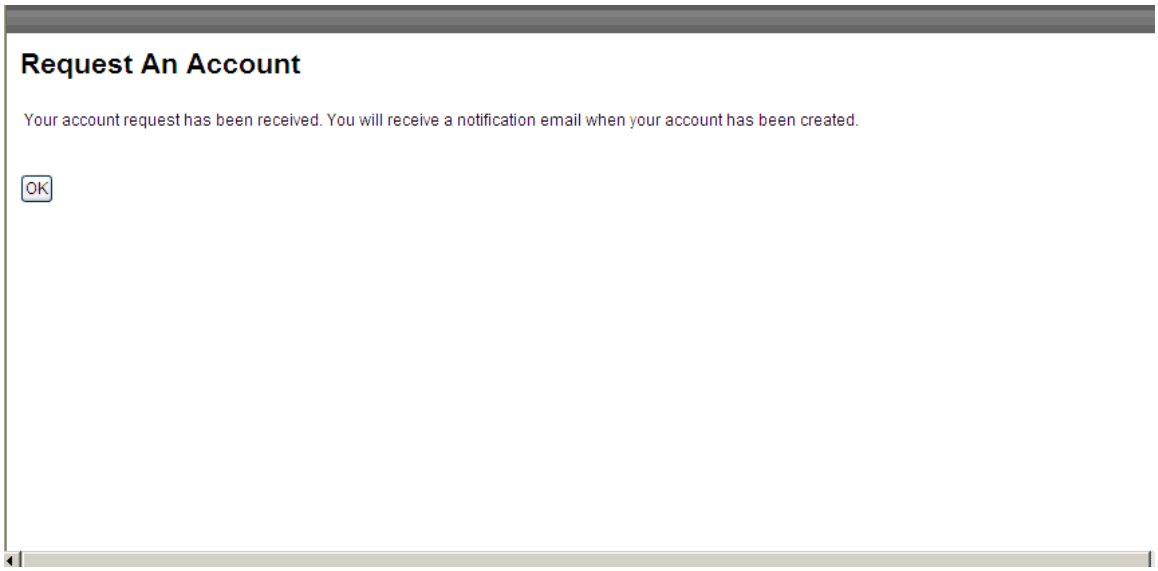

Request An Account
Basic Info
Identity Info
Business Info
Birth Date
mm/dd/yyyy
*
Identification Used
State Issued Identification Card
*
State
*
State ID Number
*
Expiration Date
mm/dd/yyyy
*
Personal Address 1
*
Personal Address 2
City
*
State
*
Zip Code
*
-
* indicates a required field
Save
Cancel


Request An Account
Basic Info
Identity Info
Business Info
Birth Date
mm/dd/yyyy
*
Identification Used
Passport
*
Country
Select Issuing Country
*
Passport Number
*
Expiration Date
mm/dd/yyyy
*
Personal Address 1
*
Personal Address 2
City
*
State
*
Zip Code
*
-
* indicates a required field
Save
Cancel


Request An Account
Basic Info
Identity Info
Business Info
Birth Date
mm/dd/yyyy
Identification Used
Permanent Resident Card
Country
Select Country of Birth
Permanent Resident Card Number
Expiration Date
mm/dd/yyyy
Personal Address 1
Personal Address 2
City
State
Zip Code
* indicates a required field
Save
Cancel


Request An Account
Basic Info
Identity Info
Business Info
Job Title
Email Address
Preferred TFA Method
Phone Number
Phone Number
Country Code
Ext.
Cell Phone Number
Country Code
Fax Number
Business Name
Select a Network
Business Address 1
Business Address 2
City
State
Zip Code
* indicates a required field


Basic Info
Identity Info
Business Info
Job Title
Web Developer
Email Address
jsmith@demo.com
Preferred TFA Method
Phone Number
Phone Number
212
112
2134
Country Code
1
Ext.
123
Cell Phone Number
347
234
6765
Country Code
1
Fax Number
212
222
3333
Business Name
Network15
Business Number
NY-2837 Coney Island Hospital
Manager Name
Select Manager
Security Official
Select Security Official
Business Address 1
Business Address 2
City
State
Zip Code


Request An Account
Your account request has been received. You will receive a notification email when your account has been created.
OK

Account Information
Part A

Specify the type of account that is being requested. If requesting a Security Official Account this form must be signed by a Notary of

*** Type of Request:**	▌ **Create New User Account**	☐ **Create Security Official Account**
	☐ **Facility** ☐ **Contractor** ☐ **Network** ☐ **CMS** ☐ **Manager** ☐ **Provider** ☐ **QIO**	☐ **SO1 (Top Level) [CMS, IT Contractor]** ☐ **SO2 (Mid-Level, Network or QIO)** ☐ **SO3 (Lowest Level) [Facility, Provider, organizational level]**

*** Date Requested:** (mm/dd/yyyy)	*** QIMS User ID:** (for Change/Disable/Enable)

Personal Information

(Per NIST 800-63, Table 3, Level 3 the applicant must be seen in person and provide a government issued picture ID such as Drivers License with current address or Passport with nationality)

Prefix:	*** First Name:**	*** Middle Name:**	*** Last Name:**	**Suffix:**
*** Personal Address 1:**		*** City:**	*** State:**	
Personal Address 2:		*** Zip Code 1:**	**Zip Code Extension:**	*** Birth date:** (mm/dd/yyyy)
*** Business Phone:**		*** Cell/2nd Phone:**	***Business E-mail Address** (if none use personal e-mail address)	
Extension:		**Extension:**		
*** Government Identification Used:** (specify type)		*** ID Number:** (specific to the ID)		
*** Issued By:** (state, country)		*** Expiration Date:** (mm/dd/yyyy)		

Business Information

*** Business Name:**		
*** Job Title:**		
*** Business Address 1:**	*** City:**	**Fax Number:**
Business Address 2:	*** Zip Code 1:**	**Zip Code Extension:**
*** Your Manager's Name:**	*** Your Manager's Email Address:**	*** State:**
*** Your Manager's Job Title:**	*** Your Manager's Phone Number:** **Ext:**	

Signatures

My statements on this form are true, complete, and correct to the best of my knowledge and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both. (See section 1001 of Title 18, United States Code). I agree to the terms and conditions documented on Page 5 of this form.	***Signature of Applicant**	*** Date:** (mm/dd/yyyy)

Account Information (continued)

Part A			
Authorization: I acknowledge that our organization is responsible for all resources to be used by the Applicant/User identified on Page 1 and that requested accesses are required to perform his or her duties. I have reviewed and verified the information supplied is accurate and appropriate. I understand that any change in employment status or access needs must be reported immediately to both (1) our designated Security Official and (2) the Help Desk.	*** Signature of Manager:**		*** Date:** (mm/dd/yyyy)
Validation: I am attesting to the fact, that I have vetted the identification of the applicant requesting access to QIMS. The individual has provided the proper credentials as required per "NIST 800-63 Table 3, Level 3**"** and I have properly identified the credential used in the "Identification Used" section. By doing so, I am attesting to the fact that I properly vetted the identity of the applicant and he/she is in fact, the applicant requesting access. I understand that any change in name, employment status or access needs must be reported immediately to both (1) our designated Security Official and (2) the Help Desk.	*** Signature of Identity Vetting Official:** (Security Official)		*** Date:** (mm/dd/yyyy)
*** Printed Name of Notary** (* Required for Security Official account only)	*** Signature of Notary**		***Date:** (mm/dd/yyyy)
***Notary Seal/Stamp**			
***Application(s) to be accessed once approved**	☐ **QIMS** ☐ **MIS** ☐ **SDPS** ☐ **QIES** ☐ **QMIS** ☐ **QualityNet.org** ☐ **PQRI** ☐ **ESRD/CROWNWeb**		
2nd Factor Credential Required? (to be filled out by the Security Official)	**Yes** ☐ **No** ☐		
Preferred 2nd Factor Contact (select one):	**Primary**	**Secondary**	**Secondary**
(Only select these options if your application requires Multi-Factor Authentication)	☐ **Business Phone** ☐ **Cell/ 2nd Phone**	☐ **Business Phone** ☐ **Cell/2nd Phone**	☐ **Business Phone** ☐ **Cell/2nd Phone**
Reason(s) for CROWNWeb account Activation Denial		☐ **Missing required * information** ☐ **Notarization** ☐ **Roles and/or scope**	

Instructions and Form Routing

INSTRUCTIONS AND FORM ROUTING for Part A:

For Type of Request = **Create New** User Account: The Applicant will fill in the on line registration form and submit it to the End User Manager (EUM) who will approve the new user for account creation and identity verification hereafter called "identity proofing". The Applicant will take part A of this form to the appointed Security Official (SO) where the Applicant will be required to perform Security Awareness Training and will undergo identity proofing. If the Applicant does not know who the assigned SO is, they can check with their EUM; or call the CROWN Help Desk at 1-888-ESRDHD1(1-888-377-3431) or send an e-mail to
support@crownhelpdesk.com

- . The Applicant must provide the registration form to the SO in person so the SO can act as the Identity Proofer. The Applicant may retain a copy of the original request form for his or her personal records.
- Note: the End User Manager will be a pre-designated for the Facility, CROWN Help Desk, network, QIO or CMS activity that the Applicant is closest to.
- Choosing an endpoint for receipt of the 2nd factor PIN is key to accessing any application that works with Protected Healthcare Information (PHI) or Personally Identifiable Information (PII). Please select an option that is close to your computer workstation as you will want easy access to the PIN that is sent via your selected method of receipt.
- Upon receipt of part A of the original form, the designated SO will review the form to ensure it is complete and will then vet the user's identity using a currently valid government picture identification document that lists the applicants current home address, or a passport showing the applicants nationality per NIST 800-63, Table 3, Level 3 E-Authentication recommendations. The SO will enter his/her name, and signature where designated on Part A of the form.
- Once identity vetting is complete, the SO will verify that the person requesting an account has completed the required Security Awareness Training (SAT). The SO will then log into QIMS and ensure the new user account is set up and assign the account holder to the proper QIMS role(s). Once the account has been set up the SO will send a fax copy to the secure fax number at the CROWN Helpdesk and then mail the original form to the CROWN Helpdesk for mandated record keeping. All forms will be mailed in tamper-resistant packaging using United States Postal Service (USPS) Certified Mail with return receipt. It is a violation of Federal security regulations to transmit any form(s) electronically; email, the Internet, unsecure transmission media, or any unsecured FAX.
- For Type of Request = **Create Security Official** Account: The Applicant will fill out the registration form, Print it out and take it to a Notary of the Public for Identity proofing.
- After the EUM has signed the form, ensured the SO Applicant has undergone Security Awareness Training and verified the information on the registration form is correct the SO will then log into QIMS and ensure the new user account is set up. The SO will then assign the account holder to the proper QIMS role(s). Once the account has been set up the SO will send a fax copy to the secure fax number at the CROWN Helpdesk and mail the original form to the CROWN Helpdesk for mandated record keeping. All forms will be mailed in tamper-resistant packaging using United States Postal Service (USPS) Certified Mail with return receipt. It is a violation of Federal security regulations to transmit any form(s) electronically; email, the Internet, unsecure transmission media, or any unsecured FAX.